## I.Vinogradov

# FUNDAMENTOS DE LA TEORIA DE LOS NUMEROS





EDITORIAL MIR

# И. Виноградов

# ОСНОВЫ ТЕОРИИ ЧИСЕЛ

### I.Vinográdov

# FUNDAMENTOS DE LA TEORIA DE LOS NUMEROS



Traducido del ruso por Candidato a doctor en ciencias físico matemáticas, catedrático de matemáticas superiores E. Aparicio Bernardo Impreso en la URSS

Segunda edición

#### **PROLOGO**

# RESEÑA BIOGRAFICA dedicada al 80 aniversario del nacimiento del académico I. M. Vinográdov

El autor de este libro, Iván Matvéevich Vinográdov (nacido el 14 (2) de Septiembre de 1891), es uno de los más célebres matemáticos de la actualidad. Las investigaciones de I. M. Vinográdov están directamente ligadas a los estudios de la escuela de teoría de los números de Petersburgo, a la cual pertenecieron P. L. Chébishev (1821-1894), E. I. Zoiotariov (1847-1878), C. F. Voronoy (1868-1908) y otros eminentes matemáticos.

El desarrollo de la teoría analítica de los números en la URSS durante los últimos 50 años está estrechamente relacionado con el nombre de Vinográdov y su escuela. Actualmente se han publicado más de 140 trabajos científicos de I. M. Vinográdov, entre los cuales merecen especial atención las monografías fundamentales: «Un método nuevo en la teoría analítica de los números» (año 1937) y «Método de las sumas trigonométricas en la teoría de los números» (año 1947). En estas dos monografías se condensan los resultados de todas las investigaciones anteriores del autor, que contribuyeron a la creación de un nuevo

método en la teoria de los números. En la actualidad, éste se conoce como el método de Vinográdov de las sumas trigonométricas. Los fundamentos de este método fueron creados ya por él mismo en el año 1934. Este es un método muy general, muy profundo y sumamente fecundo, mediante el cual I. M. Vinográdov consiguió resolver los problemas clásicos de Goldbach, Waring y otros más. En las monografias de I. M. Vinográdov desempeña un papel decisivo la acolación de las sumas trigonométricas múltiples, cuya introducción y estudio representaba de por sí un éxito de grandisima importancia en la teoria de los números. Una de estas acotaciones viene expuesta en el presente libro (véase la pregunta 14 del capítulo VI).

En esta reseña no tenemos posibilidad de hacer una exposición detallada de la obra científica de 1. M. Vinogràdov. Nos limitaremos solamente a enunciar algunos de sus resultados fundamentales.

En el año 1917, 1. M. Vinográdov se dedica al problema del cálculo asintótico de los puntos enteros dentro de los circuitos (véanse en el cap. 11, las preguntas 1 a, b, c, d, e, 22 a, b y en el cap. 111, las preguntas 5, 6). En su tiempo se ocupó de estos problemas G. F. Voronoy. Los resultados que obtuvo Voronoy para un caso particular (la hipérbola), los consiguió también Vinográdov para una clase muy amplia de circuitos, basándose en unas ideas geométricas más claras y empleando unos métodos analíticos más sencillos. En el año 1926, el matemático checo V. Yarnik demostró que estos teoremas no podían mejorarse

considerablemente. En el año 1963, 1. M. Vinográdov obtuvo también el resultado más exacto respecto del número F de puntos enteros en la esfera  $x^a + y^a + z^b \leqslant a^a$ . Este número se expresa por la fórmula asintótica

$$F = \frac{4}{3} \pi a^3 + O(a^{4/3} (\ln a)^6).$$

Algunos de los resultados de 1. M. Vinográdov ya son clásicos. Por ejemplo, ya en el año 1918 demostró que la raiz primitiva minima de un número primo p>3 (sobre las raices primitivas, véase el cap. VI, § § 1-5 y las preguntas del mismo capítulo, 5, 12 c, 14) no es superior a  $2^{th}$   $\sqrt{p}$  In p, donde h denota la cantidad de divisores primos distintos de p-1.

Es bien conocido también el siguiente teorema de I. M. Vinográdov (año 1926). Sea p un número primo y sea n un divisor de p-1, donde  $n \neq 1$ . Entonces, el no-resto mínimo de grado n respecto del módulo p (véanse los conceptos de resto y noresto en el cap. V, § 1, preguntas 8 d, 12 b y en el cap. VI, § 5) no es superior a  $p^{\frac{1}{2k}}$  (in p)³, donde  $k=e^{1-\frac{1}{n}}$ . En relación con esto, obsérvese que en el año 1796 Gauss demostró que el no-resto cuadrático mínimo (mód. p) no es superior a  $2\sqrt{p}$ . El resultado de Vinográdov fue el primer adelanto en esta cuestión desde los tiempos de Gauss.

Mucha atención prestó 1. M. Vinográdov al problema de la resolución de la ecuación  $x_1^n + \ldots + x_r^n = N$  en números enteros  $x_1 \ge 0$  (el llamado problema de Waring, planteado por éste en el año 1770). En el año 1909, D. Hilbert demuestra que esta

ecuación es resoluble para valores acolados de r. En los años 1919-1920, Hardy y Littlewood estudiaron el comportamiento asintótico del número de soluciones de las ecuaciones de Waring para  $r \ge n$   $2^m$ . El valor mínimo de r, para el cual la ecuación de Waring admite solución para todos los números N suficientemente grandes, se denota mediante G(n). Para esta magnitud, en el año 1934, I. M. Vinográdov obtuvo la cota G(n) < n (S(n n + II)) y en el año 1959, la cota más exacta G(n) < n (S(n n + II)) y en el año 1959, la cota más exacta G(n) < n (S(n n + II)) y en el año 1959, la cota más exacta S(n) < n (S(n n + II)) y en el año 1959, la cota más exacta S(n) < n (S(n) > n). Estas cotas no pueden mejorarse considerablemente, puesto que es sabido que S(n) > n ( $n \ge 2$ ).

1. M. Vinográdov demostró también que la fórmula asintótica, propuesta por Hardy y Littlewood,

$$I(N) = \frac{(\Gamma(1+v))^r}{\Gamma(rv)} N^{rv-1} \sigma + O(N^{rv-1-vs})$$

( $\mathbf{v} = \frac{1}{n}$ ,  $\Gamma$  (s) es la función Gamma de Euler;  $\sigma$  es «la serie especial», introducida por Hardy y Littlewood) para la cantidad de expresiones del número entero N > 0 en la forma  $N = x_1^n + \ldots + x_r^n$ , con enteros positivos  $x_1, \ldots, x_r$  es válida para  $r > \{10n^3 \ln n\}$ .

1. M. Vinográdou obtuvo una serie de cotas importantes: para las sumas de Weil, de la forma  $S = \sum_{x=1}^{p} \exp 2\pi i m F(x)$ , donde m > 0 es un número entero y F(x) es un polinomio de coeficientes reales; para las sumas extendidas a números primos,

de la forma  $\sum_{p < N} \exp(2\pi i\alpha p)$ , donde  $\alpha$  es un número real; para las sumas de la forma  $\sum_{p < N} \chi(p+k)$ , donde  $\chi$  denota un carácter no principal (véase la definición de carácter en el cap. VI, pregunta 9), y también en la teoria de la aproximación de polinomios mediante partes fraccionarias.

En general, es dificil indicar problemas de la teoria analítica de los números, a los cuales I M Vinográdov no haya prestado atención alguna. Por otra parte, algunos de los problemas resueltos por I M Vinográdov hablan sido ya planteados más de 150 años atrás, sin encontrar resolución alguna durante dichos años, a pesar de los esfuerzos realizados para resolverlos por los científicos más notables del mundo. Tales son, por ejemplo, los problemas de Waring u Goldbach mencionados anteriormente Este último problema apareció en el año 1742 en la correspondencia entre Chr. Goldbach y L. Euler Chr. Goldbach manifestó la hipólesis de que todo número entero, mayor que tres, podía expresarse en forma de una suma de no más de tres números primos. Todos los intentos de los grandes matemáticos de resolver este problema resultaban inútiles. En lo fundamental, este problema fue resuelto por primera vez por I. M. Vinográdov en el año 1937, demostrando que todo número impar, mayor que cierto número No (la constante de Vinográdov), se expresa en forma de una suma de no más de tres números primos. También demostró que el número de expresiones I (N) de un número impar N > 0 en forma de una suma de tres números primos,

 $N = p_1 + p_2 + p_3$ , se expresa por la fórmula asintólica  $I(N) = \frac{N^2}{2r^3}S(N) + O\left(\frac{N^2}{r^3.5-4}\right)$ ,

donde S(N) > 0.6,  $r = \ln N$  y  $\epsilon > 0$  es un número arbitrariamente pequeño. Para la constante de Vinográdov, los matemáticos soviéticos ya han demostrado que

$$N_0 \leqslant \exp \exp (16,038)$$
.

Son importantes (ambién los resultados obtenidos por 1 M. Vinográdov respecto de la ζ-función de Riemann (véase la definición en el cap. 11, preguntas 12-14,20). 1. M. Vinográdov demostró que

$$\zeta(l+it) = O((\ln t)^{2/3})$$

y que  $\zeta$  (1 + i1) no tiene ceros en la región

$$\sigma > 1 - \frac{A}{(\ln t)^{2/3}}.$$

Para la cantidad de números primos  $\pi$  (x) que no son superiores a x (véase el cap. 11, preguntas 19c, 24), de aqui resulta la acolación

$$\pi(x) = \int_{2}^{\pi} \frac{dx}{\ln x} + O\left(xe^{-\alpha(\ln x)^{0.0}}\right),$$

donde  $\alpha > 0$  es una constante.

Los métodos de Vinográdov fueron desarrollados también, y siguen desarrollándose actualmente, por sus numerosos alumnos, de los cuales en esta breve reseña no tenemos posibilidad de relatar.

Para concluir, indiquemos que desde el año 1932 1. M. Vinográdov encabeza el centro matemático principal de la Unión Soviética, el Instituto Matemático V. A. Steklov de la Academia de Ciencias de la URSS. I. M. Vinográdov es miembro numerario de la Academia de Ciencias de la URSS desde el año 1929.

Los méritos de I. M. Vinográdov en la teoría de los números también han sido reconocidos como corresponde fuera de la Unión Soviética. I. M. Vinográdov es miembro extranjero de la Sociedad Real de Londres, de la Academia de Ciencias de Dinamarca y de la Academia Nacional dei Lincei (Roma); es miembro honorifico de la Academia de Ciencias de Hungria; es miembro correspondiente de la Academia de Ciencias de Alemania en Berlin y de la Academia de Ciencias de Paris; es Doctor honorifico de filosofía de la Universidad de Oslo (Noruega); es miembro extranjero honorifico de las Sociedades Matemáticus de Amsterdam, Londres y de la India, así como de la Sociedad Filosófica americana en Filadelfia y de la Academia americana de Artes y Ciencias en Bostón.

El libro que proponemos, «fundamentos de la teoría de los números», a distinción de otras obras de 1. M. Vinográdov, es un manual de texto destinado a los estudiantes de las facultades de matemáticas de las universidades. Es dificil hallar otro libro tan conciso sobre teoría de los números, donde el material esté expuesto con tanta claridad y rigurosidad.

En lo fundamental, está dedicudo al estudio de la tevria de las congruencias. No obstante, las preguntas expuestas al final de cada capitulo abarcan un material que está relacionado

ya con los problemas fundamentales de la teoría analítica de los números.

Durante la preparación de la traducción castellana, el autor expuso al traductor su opinión acerca de la utilización del libro por el lector. El autor considera que al preparar las respuestas a las preguntas, primero hay que hacer la prueba de resolver los problemas planteados individualmente. Solamente cuando se hayan agotado todos los medios para su resolución, el lector deberá examinar las respuestas e indicaciones que se dan al final del libro.

El presente libro «fundamentos de la teoría de los números», fue escrito sobre la base de los cursos explicados por el autor en tos años 1918-1920 en la Universidad de Perm y en los años 1920-1934 en la Universidad de Leningrado. La primera edición del libro salió en el año 1936. En adelante, el libro ha sido mejorado y completado. La presente traducción se ha hecho de la séptima edición rusa

25. XII. 1970

E APARICIO BERNARDO

#### CAPITULO PRIMERO

#### Teoría de la divisibilidad

§ 1. Conceptos a. La teoría de los números se dedica al y teoremas estudio de las propiedades de los números fundamentales enteros. Llamaremos enteros no sólo a los números de la serie natural 1, 2, 3, . . . (enteros positivos), sino también al cero y a los enteros negativos —1, —2, —3, . . .

Por regla general, al exponer la teoría designaremos con letras solamente los números enteros. Los casos en que las letras no designen números enteros los advertiremos especialmente, si es que ello mismo no está claro.

La suma, diferencia y producto de dos enteros a y b también serán enteros, pero el cociente de la división de a por b (si b es distinto de cero) puede ser tanto entero como no entero

b. Si el cociente de la división de a por b es entero, designándole con la letra q, se tiene a=bq, es decir, a es igual al producto de b por un entero. Diremos entonces que a es divisible por b o que b divide a a. En este caso, a se llama múltiplo de b y b se llama divisor de a. El hecho de que b divide a a se escribe así  $b \setminus a$ .

Subsisten los dos teoremas siguientes:

1. Si a es múltiplo de m y m es múltiplo de b, a es multiplo de b.

En efecto, de  $a - a_1 m$ ,  $m = m_1 b$  se deduce que  $a = a_1 m_1 b$ , donde  $a_1 m_1$  es entero. Esto demuestra el teorema.

2. Si en una igualdad de la forma k+l+...+n p+q+...+s, respecto de todos los términos, a excepción de uno cualquiera de ellos, se sabe que son múltiplos de b, entonces este término también es múltiplo de b
En efecto, sea k tal término. Se tiene

$$l = l_1 b_1 \dots n_1 b_1 \ p = p_1 b_1 \ q = q_1 b_2 \dots s = s_1 b_1$$
  
 $k = p + q + \dots + s + l - \dots - n = s_1 b_2$   
 $= (p_1 + q_1 + \dots + s_1 - l_2 + \dots + n_1) b_2$ 

Esto demuestra el teorema.

c. En el caso general, que incluye particularmente el caso en que a es divisible por b, se tiene el teorema:

Todo entero a se expresa de un módo único mediante un entero positivo b en la forma

$$a = bq + r; 0 \leqslant r \leqslant t$$

En efecto, se obtiene una expresión de a en tal forma tomando bq igual al máximo múltiplo del número b que no es superior a a. Suponiendo que también  $a - bq_1$  (  $r_1$ ,  $0 \le r_1 \le b$ , resulta 0 = b ( $q - q_1$ )  $+ r - r_2$ , de donde se deduce (2, b) que  $r - r_4$  es múltiplo de b. Pero en vírtud de $|r - r_1| < b$ , lo último es posible solamente si  $r - r_1 = 0$ , es decir, si  $r = r_1$ , de donde se deduce también que  $q = q_1$ .

El número q se llama cociente incompteto y el número r, residuo o resto de la división de a por b.

**Ejemplo.** Sea b = 14. Se tiene

$$177 = 14 \cdot 12 + 9;$$
  $0 < 9 < 14.$   
 $-64 \cdot 14 \cdot (-5) + 6;$   $0 < 6 < 14,$   
 $154 = 14 \cdot 11 + 0;$   $0 = 0 < 14.$ 

8 2. Máximo comán divisor

a. A continuación consideraremos sólo los divisores positivos de los números. Todo entero que divide simultáneamente a los enteros a, b, . . . , l, se llama divisor común de los mismos. El mayor de los divisores comunes se llama máximo común divisor y se designa con la notación (a, b, . . . . l). Como la cantidad de divisores comunes es finita, la existencia del máximo común divisor es evidente. Si  $(a, b, \ldots, l) = 1$ , a, b, ..., l se llaman primos entre sí. Si cada uno de los números a, b, . . . , l, es primo con cada uno de los demás, a, b, . . . . I se llaman primos entre si dos a dos. Es obvio que los

Elempios. Como (6, 10, 15) = 1, los números 6, 10, 15 son primos entre si. Como (8, 13) = (8, 2i) = (13, 21) = 1, los números 8, 13, 21 son primos entre sí dos a dos.

números primos entre si dos a dos son también primos entre si: en el caso de dos números los conceptos de «primos entre

si dos a dos» y eprimos entre sia coinciden.

b. Ocupémonos primero de los divisores comunes de dos números.

1. Si a es múltiplo de b. el conjunto de los divisores comunes de los números a y b coincide con el conjunto de los divisores del solo número b; en particular, (a, b) = b,

En efecto, todo divisor común de los números a v b es un divisor de b. Reciprocamente, siendo a múltiplo de b. todo divisor del número b (1, b, & 1) es también un divisor del número a, es decir, es un divisor común de los números b y a. Por lo tanto, el conjunto de los divisores comunes de los números a y b coincide con el conjunto de los divisores del solo número b. Y como el máximo divisor del número b es el mismo b, resulta (a, b) - b.

2. Si a = ba + c.

entonces el conjunto de los divisores comunes de los números a y b coincide con el conjunto de los divisores comunes de los números b u c. en particular, (a, b) - (b, c).

En efecto, la igualdad escrita más arriba muestra que todo común divisor de los números a y b divide también a c  $(2, b, \frac{a}{2}, 1)$  y, por consiguiente es un común divisor de los números b y c. Recíppocamente, la misma igualdad muestra que todo común divisor de los números b y c divide a a y, por consiguiente, es un común divisor de los números a y b. Por lo tanto, los divisores comunes de los números a y b son los mismos que los divisores comunes de los números a y a0 en particular, tienen que coincidir también los mayores de estos divisores, es decir, a0 a0 a0 a0 a0.

c. Para buscar el máximo común divisor, así como para deducir sus propledades principales, se emplea el algoritmo de Euclides Este último consiste en lo siguiente. Sean a y b enteros positivos. Según c, § 1, hallamos la serie de igualdades:

$$a = bq_1 + r_2, \qquad 0 < r_2 < b,$$

$$b = r_2q_3 + r_3, \qquad 0 < r_3 < r_3,$$

$$r_2 = r_3q_3 + r_4, \qquad 0 < r_4 < r_3,$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \qquad 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_nq_n,$$

$$r_{n-1} = r_nq_n,$$

$$r_{n-1} = r_nq_n,$$

$$r_{n-2} = r_nq_n,$$

$$r_{n-1} = r_nq_n,$$

$$r_{n-2} = r_nq_n,$$

$$r_{n-3} = r_nq_n,$$

$$r_{n-4} = r_nq_n,$$

$$r_{n-4} = r_nq_n,$$

que termina cuando se obtiene cierto  $r_{n+1}=0$ . Esto último es indispensable, puesto que la sucesión  $b, r_2, r_3, \ldots$ , como sucesión de enteros decrecientes, no puede contener más de b positivos.

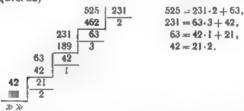
d. Examinando las igualdades (1) de arriba a abajo, nos convencemos (b) de que los divisores comunes de los números a y b son iguales a los divisores comunes de los números b y  $r_3$ , luego son iguales a los divisores comunes de los números  $r_2$  y  $r_3$ , de los números  $r_3$  y  $r_4$ , . . . , de los números  $r_{n-4}$  y  $r_n$ , finalmente, a los divisores del solo número  $r_n$ . A la vez, se tiene

$$(a, b) - (b, r_2) = (r_2, r_3) - \ldots = (r_{n-1}, r_n) = r_n.$$

Obtenemos los siguientes resultados.

- El conjunto de los divisores comunes de los números a y b coincide con el conjunto de los divisores de su máximo común divisor.
- 2. Este máximo común divisor es igual a r<sub>n</sub> es decir, es igual al último resto del algoritmo de Euclides, distinto de cero.

Ejempto. Apliquemos el algoritmo de Euclides para averiguar (525, 231). Hallamos (los cálculos auxiltares se exponen a la izquierda)



Aqui el último resto positivo es  $r_4 = 21$ . Por lo tanto, (525, 231) = 21.

- e. 1. Designando con la letra m cualquier entero positivo, se tiene (am, bm) ... (a, b) m.
- 2. Designando con la letra  $\delta$  cualquier divisor común de los números a y b, se tiene  $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a, b)}{\delta}$ ; en particular, se tiene  $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$ , es decir, los cocientes de la división de dos números por su máximo común divisor son números primos entre si.

En efecto, multipliquemos las relaciones (1) término a término por m. Obtendremos nuevas relaciones, donde en lugar de  $a, b, r_2, \ldots, r_n$  figurarán  $am, bm, r_2m, \ldots, r_nm$ . Por esto,  $(am, bm) = r_nm$ , y por lo tanto, el aserto 1 es cierto. Aplicando el aserto 1, hallamos

$$(a, b) = \left(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\right) = \left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta,$$

de donde se deduce el aserto 2.

1. 1. Si(a, b) = 1, so tiene (ac, b) = (c, b).

En efecto, (ac, b) divide a ac y bc y, por consiguiente, (1, d), también divide a (ac, bc), igual a c, debido a 1, e; pero (ac, b) divide a b, por lo cual también divide a (c, b). Reciprocamente, (c, b) divide a ac y b, por lo cual también divide a (ac, b). Por lo tanto, (ac, b) y (c, b) se dividen mutuamente y, por consiguiente, son iguales entre sí.

2. Si (a, b) = 1 y ac es divisible por b, entonces c es divisible por b.

En efecto, de (a, b) = 1 y de 1 se deduce que (ac, b) = (c, b), y de la divisibilidad de ac por b y de 1, b se deduce que (ac, b) = b. Por esto (c, b) = b y, por consiguiente, c es divisible por b.

3. Si cada uno de los números  $a_1, a_2, \ldots, a_m$  es primo con cada uno de los números  $b_1, b_2, \ldots, b_n$ , el producto  $a_1, a_2, \ldots, a_m$  es primo con el producto  $b_1, b_2, \ldots, b_n$ .

En efecto, (teorema 1), se tiene

$$(a_1a_3a_3 \ldots a_m, b_k) = (a_2a_3 \ldots a_m, b_k) =$$
  
=  $(a_3 \ldots a_m, b_k) = \ldots = (a_m, b_k) = 1$ ,

y haciendo luego para abreviar  $a_1a_2\ldots a_m-A$ , hallamos del mismo modo

$$(b_1b_2b_3...b_n, A) = (b_2b_3...b_n, A) =$$
  
=  $(b_3...b_n, A) = ... = (b_n, A) = 1.$ 

g. El problema de la averiguación del máximo común divisor de más de dos números se reduce al mísmo para dos números. Precisando, para hallar el máximo común divisor de los números  $a_1, a_2, \ldots, a_n$ , formamos la sucesión de números:

$$(a_1, a_2) = d_2, (d_3, a_3) = d_2, (d_3, a_4) = d_4,$$
  
 $\dots, (d_{n-1}, a_n) = d_n.$ 

El número  $d_n$  será el máximo común divisor de todos los números dados.

En efecto, (1, d), los divisores comunes de los números  $a_1$  y  $a_2$ 

coinciden con los divisores de  $d_2$ ; por esto, los divisores comunes de los números  $a_1$ ,  $a_2$  y  $a_3$  coinciden con los divisores comunes de los números  $d_3$  y  $a_3$ , es decir, coinciden con los divisores de  $d_3$ . Luego nos convencemos de que los divisores comunes de los números  $a_1$ ,  $a_2$ ,  $a_3$ ,  $a_4$  coinciden con los divisores de  $d_4$ , etc., y, finalmente que los divisores comunes de los números  $a_1$ ,  $a_2$ , ...,  $a_n$  coinciden con los divisores de  $d_n$ . Y como el mayor divisor de  $d_n$  es el mismo  $d_n$ , éste será el máximo común divisor de los números  $a_1$ ,  $a_2$ , ...,  $a_n$ .

Examinando la demostración expuesta nos convencemos de que el teorema 1, d subsiste también para más de dos números. Subsisten también los teoremas 1, e y 2, e, puesto que al multiplicar por m o al dividir por  $\delta$  todos los números  $a_1$ ,  $a_2$ , . . . ,  $a_n$  también se multiplican por m o se dividen por  $\delta$  todos los números  $d_3$ ,  $d_3$ , . . . ,  $d_n$ .

#### § 3. Minimo común máitipio

a. Todo entero que es un múltiplo de todos los números dados se llama múltiplo común de los mismos. El menor múltiplo común positivo se llama mínimo común múltiplo.

b. Ocupémonos primero del mínimo común múltiplo de dos números Sea M algún múltiplo común de los enteros a y b. Como éste es múltiplo de a, se tiene M=ak, donde k es entero. Pero M también es múltiplo de b, por lo cual también tiene que ser entero

el cual, haciendo (a, b) = d,  $a = a_1d$ ,  $b = b_1d$ , se puede expresar en la forma  $\frac{a_1k}{b_1}$ , donde  $(a_1, b_1) = 1$  (2, e, § 2). Por esto (2, f, § 2), k tiene que ser divisible por  $b_1$ ,  $k = b_1t = \frac{b}{d}t$ , donde t es entero. De aqui que

$$M = \frac{ab}{d}t$$
.

Reciprocamente, es evidente que cualquier M de esta forma es múltiplo tanto de a como de b, y, por consiguiente, esta forma proporciona todos los múltiplos comunes de los números a y b.

El menor positivo de estos múltiplos, es decir, el mínimo común múltiplo, se obtiene para t = 1. Este es

$$m=\frac{ab}{d}$$
.

Introduciendo m, la fórmula obtenida para M se puede escribir así:

$$M = mt$$
.

La última y penúltima igualdades dan lugar a los teoremas:

1. El conjunto de los múltiplos comunes de dos números coincide con el conjunto de los múltiplos de su mínimo común múltiplo.

2. Este minimo común múltiplo de dos números es igual a su

producto, dividido por su máximo común divisor.

c. Supongamos que se necesita hallar el mínimo común múltiplo de más de dos números  $a_1, a_2, \ldots, a_n$ . Designando en general con la notación (a, b) el mínimo común múltiplo de los números  $a \ y \ b$ , formemos la sucesión de números:

 $[a_1, a_2] = m_2, [m_2, a_3] = m_3, \ldots, [m_{n-1}, a_n] = m_n.$ 

El número  $m_n$  obtenido de este modo será el mínimo común

múltiplo de todos los números dados.

En electo, (1, b), los múltiplos comunes de los números  $a_1$  y  $a_2$  coinciden con los múltiplos de  $m_2$ , por lo cual los múltiplos comunes de los números  $a_1$ ,  $a_2$ , y  $a_3$  coinciden con los múltiplos comunes de  $m_2$  y  $a_3$ , es decir, coinciden con los múltiplos de  $m_3$ . Luego nos convencemos de que los múltiplos comunes de los números  $a_1$ ,  $a_2$ ,  $a_3$ ,  $a_4$  coinciden con los múltiplos de  $m_4$ , etc., y, finalmente, de que los múltiplos comunes de los números  $a_1$ ,  $a_2$ , ...,  $a_n$  coinciden con los múltiplos de  $m_n$ , y como el menor múltiplo positivo de  $m_n$  es el mismo  $m_n$ , éste

mínimo común múltiplo de dos números a. . . . . an.

Examinando la demostración expuesta, vemos que el teorema 1, b subsiste también para más de dos números. Además, nos convencemos de que se verifica el siguiente teorema:

El minimo común múltiplo de números que son primos dos a dos es igual al producto de los mismos

#### \$ 4. Relación del algoritmo de Euclides con las fracciones continuas

a. Sea a cualquier número real Designemos con la letra quel mayor entero que no supera a a Si a no es entero, se tiene

$$\alpha = q_1 \mid \frac{1}{\alpha_2}; \alpha_2 > 1.$$

Exactamente igual, si a2, ..., as-i no son enteros, se tiene

$$a_2 \cdot q_2 + \frac{1}{a_3}, \ a_3 > 1;$$

$$a_{4-1} = q_{4-1} + \frac{1}{a_4}; \ a_4 > 1,$$

en virtud de lo cual obtenemos el siguiente desarrollo de a en fracción continua:

to cual obtenemos el siguiente desarrollo de 
$$\alpha$$
 continua:
$$\alpha = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \cdots}} + \frac{1}{q_{d-1} + \frac{1}{\alpha_d}}.$$
(1)

 b. Si α es irracional, todos los números α, son irracionales (si α, fuese racional, en virtud de (1), resultaria también α racional) y el proceso indicado puede prolongarse indefinidamente.

Si α es racional y, por consiguiente, puede expresarse por una fracción racional irreducible con denominador positivo:  $\alpha = \frac{\alpha}{h}$ , el proceso indicado será finito y puede efectuarse mediante el aigoritmo de Euclides. En efecto se tiene:

$$a = bq_1 + r_2; \qquad \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_2}},$$

$$b = r_2q_2 + r_3; \qquad \frac{b}{r^2} = q_2 + \frac{1}{\frac{r_3}{r_3}},$$

$$r_{n-2} = r_{n-1}q_{n-1} + r_n; \qquad \frac{r_{n-3}}{r_{n-1}} = q_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}},$$

$$r_{n-1} = r_nq_n; \qquad \frac{r_{n-1}}{r_n} = q_n,$$

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots}}, + \frac{1}{q_n}.$$

c. Los números  $q_1, q_2, \ldots$ , que figuran en el desarrollo del número  $\alpha$  en fracción continua, se llaman cocientes incompletos (en caso de  $\alpha$  racional, según  $\mathbf{b}$ , éstos son los cocientes incompletos de las divisiones sucesivas del algoritmo de Euclides), las fracciones

$$\delta_1 = q_1, \quad \delta_2 = q_1 + \frac{1}{q_2}, \quad \delta_3 = q_1 + \frac{1}{q_2 + \frac{1}{q_2}}, \dots$$

se llaman reducidas.

d. Fácilmente se halla una ley muy simple de formación de las reducidas, observando que  $\delta_a(s>1)$  se obtiene de  $\delta_{a-1}$  sustituyendo los números  $q_{a-1}$  por  $q_{a-1}+\frac{1}{q_a}$  en la expresión literal  $\delta_{a-1}$ . En efecto, haciendo para unificar  $P_0=1$ ,  $Q_0=0$ , podemos representar sucesivamente las fracciones reducidas en la forma siguiente (aquí se escribe la igualdad  $\frac{A}{B}=\frac{P_a}{Q_a}$ 

para designar A con la notación  $P_*$  y B con la notación  $Q_*$ ):

$$\begin{split} &\delta_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}\,, \\ &\delta_2 = \frac{q_1 + \frac{1}{q_2}}{1} = \frac{q_2q_1 + 1}{q_2 \cdot 1 + 0} = \frac{q_3P_1 + P_0}{q_3Q_1 + Q_0} = \frac{P_3}{Q_2}\,, \\ &\delta_3 = \frac{\left(q_2 + \frac{1}{q_3}\right)P_1 + P_0}{\left(q_3 + \frac{1}{q_3}\right)Q_1 + Q_0} = \frac{q_3P_3 + P_1}{q_3Q_1 + Q_1} = \frac{P_3}{Q_3}\,. \end{split}$$

etc, y, en general,

$$\delta_a = \frac{q_a P_{a-1} + P_{a-2}}{q_a Q_{a-1} + Q_{a-1}} = \frac{P_a}{Q_a}.$$

Por lo tanto, los numeradores y denominadores de las fracciones reducidas los podemos calcular sucesivamente por las fórmulas

$$\begin{cases}
P_{\bullet} = q_{\bullet} P_{\bullet-1} + P_{\bullet-2}, \\
Q_{\bullet} = q_{\bullet} Q_{\bullet-1} + Q_{\bullet-2}.
\end{cases}$$
(2)

Es útil realizar estos cálculos según el esquema siguiente (las últimas dos columnas se escriben solamente en el caso en que  $\alpha$  es una fracción irreducible con el denominador positivo:  $\alpha = \frac{a}{b}$ ):

qu q1		q <sub>1</sub>	q <sub>2</sub>	4 * *			q <sub>4</sub>		q <sub>n</sub>
Pa	1	qı	Pa	* * *	P <sub>8-1</sub>	$P_{4-1}$	Pa	$P_{h-1}$	a
$Q_{a}$	0	1	$Q_3$		$Q_{s-2}$	$Q_{s-1}$	Q <sub>4</sub>	$Q_{n-1}$	ь

**Ejemplo.** Desarrollemos en fracción continua el número  $\frac{105}{38}$ . Aguí

Por esto, el esquema indicado anteriormente da

q <sub>a</sub>		2	1	3	4	2
Pa	1	2	3	11	47	105
$Q_{\alpha}$	0	3	1	4	17	38

e. Examinemos la diferencia  $\delta_s - \delta_{s-1}$  de dos fracciones reducidas consecutivas. Para s > 1 haliamos

$$\tilde{\Phi}_{a} - \tilde{\Phi}_{s-1} = \frac{P_{a}}{Q_{a}} - \frac{P_{s-1}}{Q_{s-1}} = \frac{h_{s}}{Q_{s}Q_{s-1}}$$

donde  $h_s = P_s Q_{s-1} - Q_s P_{s-1}$ ; poniendo en fugar de  $P_s$  y  $Q_s$  sus expresiones (2) y haciendo las simplificaciones evidentes, obtenemos  $h_s = -h_{s-1}$  Esto último, junto con  $h_1 - q_1 \cdot 0 - -1 \cdot 1 = -1$  da  $h_s - (-1)^s$ . Así, pues,

$$P_s Q_{s-1} - Q_s P_{s-1} = (-1)^s (s > 0),$$
 (3)

$$\delta_s - \delta_{s-1} = \frac{(-1)^s}{Q_s Q_{s-1}}$$
 (s > 1). (4)

Ejemplo. En la tabla del ejemplo expuesto en d, se tiene  $105 \cdot 17 - 38 \cdot 47 = (-1)^a = -1$ .

f. De (3) se deduce que  $(P_s, Q_s)$  divide a  $(-1)^s = \pm 1$  (2, b,

§ 1) Por esto  $(P_a, Q_a) = 1$ , es decir, las fracciones reducidas  $\frac{P_a}{Q_a}$  son irreducibles.

g. Supongamos que  $s \gg 2$  y que  $\delta_a$  no es igual a  $\alpha$ . Las expresiones para  $\delta_{a-1}$  y para  $\delta_a$  se obtienen fácilmente de la expresión (1) para  $\alpha$ : la primera, sustituyendo  $\frac{1}{\alpha_a}$  por cero, la segunda, sustituyendo  $\frac{1}{\alpha_a}$  por el número  $\frac{1}{q_a}$ . Pero de las igualdades indicadas en a para  $\alpha_{a-1}, \ldots, \alpha_2, \alpha$ , fácilmente

at hacer
la primera
sustitución
sustitució

y que, finalmente, al hacer una de dichas sustituciones α disminuye, y al hacer la otra α aumenta. Esto último muestra

 $\delta_{i-1} y \delta_i$ h. Se tiene

comprobamos que

$$|\alpha - \delta_{t-1}| \leq \frac{1}{Q_t Q_{t-1}}$$

que uno de los números  $\delta_{s-1}$  y  $\delta_s$  es menor que  $\alpha$ , y el otro es mayor que  $\alpha$ , y que, por lo tanto,  $\alpha$  está comprendido entre

En efecto, si  $\delta_a = \alpha$  este aserto se deduce (con el signo de igualdad) de (4). Si  $\delta_a$  no es igual a  $\alpha$ , se deduce (con el signo de desigualdad) de g y de (4).

§ 8. Números a. El número I sólo tiene un divisor primos positivo, precisamente I. En este sentido el número I en la sucesión de números naturales, es particular.

Todo entero mayor que 1 tiene al menos dos divisores, precisamente 1 y él mismo; si con estos divisores se agotan todos los divisores positivos del número entero, éste se llama *prumo*. Un entero mayor que 1, que tenga además de 1 y de sí mismo otros divisores positivos, se llama *compuesto*.

b. El divisor menor, distinto de la unidad, de un entero mayor que la unidad, es un número primo.

En efecto, sea q el divisor menor, distinto de la unidad, de un entero a > 1. Si q fuese compuesto tendría un divisor  $q_1$  con la condición  $1 < q_1 < q$ ; pero el número a, siendo divisible por q, tendría que ser divisible también por  $q_1$  (1, b, q), y esto contradice a la hipótesis respecto del número a.

c. El divisor menor, distinto de la unidad, de un número compuesto a (según b, tiene que ser primo) no es superior a  $\sqrt{a}$ .

En efecto, sea q este divisor, entonces  $a = qa_1$ ,  $a_1 \ge q$ , de donde, multiplicando y simplificando por  $a_1$ , obtenemos  $a \ge q^2$ ,  $q \le \sqrt{a}$ .

d. La cantidad de números primos es infinita

La validez de este teorema se deduce de que, cualesquiera que sean los números primos distintos  $p_1, p_2, \ldots, p_h$ , se puede obtener un número primo nuevo que no está comprendido entre ellos. Tal es el divisor primo de la suma  $p_1, p_2, \ldots, p_h + 1$ , el cual, dividiendo a toda la suma, no puede coincidir con ninguno de los primos  $p_1, p_2, \ldots, p_h$  (2, b, § 1).

e. Para formar la tabla de números primos que no superan a un número dado N, existe un método sencillo, denominado

criba de Eratóstenes. Este consiste en lo siguiente.

Escribamos los números

$$1, 2, \ldots, N.$$
 (1)

El primer número de esta sucesión que es mayor que la unidad es el 2; éste sólo es divisible por 1 y por sí mismo y, por consiguiente, es primo.

Borremos de la sucesión (1) (como compuestos) todos los números que son múltiplos de 2, a excepción del mismo 2. El primer número no borrado que le sucede al 2 es el 3; éste no es divisible por 2 (pues en caso contrario estaría borrado), por lo cual 3 sólo es divisible por 1 y por sí mismo y, por consiguiente, es primo.

Borramos de la sucesión (1) todos los números que son múltiplos de 3, a excepción del mismo 3. El primer número no borrado que le sucede al 3 es el 5; éste no es divisible por 2 ni por 3 (pues en caso contrario estaría borrado). Por consiguiente, 5 sólo es divisible por 1 y por sí mismo, por lo cual, tamblén es primo. Etc.

Cuando se hayan borrado del modo indicado todos los números que son múltiplos de los números primos menores que un número primo p, todos los números no borrados, menores que  $p^s$ , serán primos En efecto, cualquier número compuesto a, menor que  $p^s$ , ya está borrado, por ser múltiplo de su divisor primo menor, el cual  $\leqslant V\overline{a} < p$ . De aquí se deduce que:

- Al comenzar a borrar los múltiplos de un número primo p, hay que empezar a borrar desde p³.
- 2. La formación de la tabla de números primos  $\leq N$  se termina en cuanto se hayan borrado todos los números compuestos que son múltiplos de los números primos que no son superiores a  $\sqrt{N}$ .
- § 6. Unicidad de la descomposición en factores primos
- a. Todo entero a, o es primo con un número primo dado p, o es divisible por p.

En efecto, (a, p), siendo un divisor de p, puede ser igual a 1 o a p. En el primer caso a es primo con p, en el segundo a

es divisible por p.

b. S<sub>i</sub> el producto de varios factores es divisible por p<sub>i</sub> al menos uno de los factores es divisible por p<sub>i</sub>. En efecto, (a), cada factor es primo con p o es divisible por p. Si todos los factores fuesen primos con p, su producto (3, f, § 2) sería primo con p; por esto, al menos uno de los factores es divisible por p.

c. Todo entero, mayor que la unidad, se descompone en un producto de factores primos y, además, de modo único, si no se tiene en cuenta el orden de los factores

En efecto, sea a un entero, mayor que la unidad; designando con la letra  $p_1$  su divisor primo menor, se tiene  $a=p_1a_1$ . Si  $a_1>1$ , designando con la letra  $p_2$  su divisor primo menor, se tiene  $a_1=p_2a_2$ . Si  $a_2>1$ , de un modo semejante se obtiene  $a_2=p_3a_3$ , etc, y así hasta que se llegue a obtener un número  $a_n$  igual a la unidad. Entonces  $a_{n-1}=p_n$ . Multiplicando todas las igualdades obtenidas y efectuando la simplificación, resulta la siguiente descomposición del número a en factores primos:

$$a = p_1 p_2 \dots p_n$$

Supongamos que para el mismo número a existe también una segunda descomposición en factores primos  $a = q_1q_2 \dots$  ...  $q_s$ . Entonces

$$p_1p_2\ldots p_n=q_1q_2\ldots q_n$$

El segundo miembro de esta igualdad es divisible por  $q_1$ . Por lo tanto (b), al menos uno de los factores del primer miembro tiene que ser divisible por  $q_1$ . Supongamos, por ejemplo, que  $p_1$  es divisible por  $q_1$  (el orden de numeración de los factores está a cargo nuestro); entonces  $p_1 = q_1(p_1)$  además de l es divisible por  $p_1$ . Simplificando ambos miembros de la igualdad por  $p_1 = q_1$ , se tiene  $p_2p_3 \ldots p_n = q_3q_3 \ldots q_n$ . Repitiendo el razonamiento anterior para esta igualdad, obtenemos  $p_3 \ldots p_n = q_3 \ldots q_n$ , etc. Continuamos así hasta que al fin y al cabo en un miembro de la igualdad, por ejemplo, en el primero, se simplifiquen todos los factores. Pero simultáneamente tienen que simplificarse

también todos los factores del segundo miembro, puesto que la igualdad  $1 = q_{n+1}$  .  $q_n$  siendo  $q_{n+1}$ , . . ,  $q_n$  superiores a 1, es imposible.

Por lo tanto, la segunda descomposición en factores primos es idéntica a la primera.

d. En la descomposición del número a en factores primos algunos de ellos pueden repetirse. Designando con las letras  $p_1, p_2, \ldots, p_k$  los primos distintos que figuran en dicha descomposición y con las letras  $\alpha_1, \alpha_2, \ldots, \alpha_k$  sus órdenes de multiplicidad en a, obtenemos la llamada descomposición canónica del número a en factores:

$$a = \rho_1^{\alpha_1} \rho_2^{\alpha_2} \dots \rho_k^{\alpha_k}$$

**Ejemplo.** La descomposición canónica del número 588 000 es:  $588\,000 = 2^4 \cdot 3 \cdot 5^9 \cdot 7^2$ .

e. Sea  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  la descomposición canónica del número a. Entonces todos los divisores de a son todos los números de la forma

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}; \qquad (1)$$

$$0 \le \beta_1 \le \alpha_1, \quad 0 \le \beta_2 \le \alpha_2, \quad \dots, \quad 0 \le \beta_k \le \alpha_k.$$

En efecto, supongamos que d divide a a. Entonces (b, § 1) a-dq y, por consiguiente, todos los divisores primos de d figuran en la descomposición canónica de a con exponentes no menores que los exponentes con que ellos mismos figuran en la descomposición canónica de d. Por esto d tiene la forma (1).

Recíprocamente, todo número d de la forma (I) es, evidentemente, un divisor de a.

**Ejemplo.** Se obtienen todos los divisores del número 720 —  $= 2^4 \ 3^3 \ 5$  haciendo recorrer en la expresión  $2^{\beta_1}3^{\beta_2}5^{\beta_3}$  a  $\beta_1$ ,  $\beta_2$ ,  $\beta_3$ , independientemente unos de otros, los valores  $\beta_1 = 0$ , 1, 2, 3, 4;  $\beta_2 = 0$ , 1, 2;  $\beta_3 = 0$ , 1 Por esto, los

divisores indicados son: 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144, 5, 10, 20, 40, 80, 15, 30, 60, 120, 240, 45, 90, 180, 360, 720.

#### Preguntas referentes al capitulo l

- 1. Sean  $a \ y \ b$  enteros, no simultaneamente iguales a cero, y sea  $d = ax_0 + by_0$  el número positivo menor de la forma ax + by ( $x \ e \ y$  son enteros). Demostrar que d (a, b). Deducir de aqui el teorema 1, d, § 2 y los teoremas e, § 2 Generalizar estos resultados, considerando los números de la forma  $ax + by + \dots + fu$ .
- 2. Demostrar que la fracción reducida  $\delta_t$  representa al número  $\alpha$  con más exactitud que cualquier fracción irreducible  $\frac{k}{l}$  que cumpla la condición  $0 < l < Q_t$ .
- 8. Supongamos que el número real  $\alpha$  se ha desarrollado en una fracción continua; sea N un entero positivo, k el número de sus cifras decimales y n el entero mayor que cumple la condición  $Q_n \leq N$  Demostrar que  $n \leq 5k+1$  Para la demostración se deben comparar las expresiones para  $Q_2$ ,  $Q_3$ ,  $Q_4$ , . . . ,  $Q_n$  con las que éstos tendrían si todos los  $q_a$  fuesen iguales a 1, y comparar luego con los números 1,  $\xi$ ,  $\xi^n$ , . . . ,  $\xi^{n-1}$ , donde  $\xi$  es la raíz positiva de la ecuación  $\xi^a = \xi + 1$ .
- 4. Sea  $\tau \geqslant 1$ . Una sucesión de fracciones racionales irreducibles, dispuestas en orden de crecimiento, con denominadores positivos no superiores a  $\tau$ , se llama sucesión de Farey correspondiente a  $\tau$ .
- a. Demostrar que la parte de la sucesión de Farey correspondiente a  $\tau$ , que contiene fracciones  $\alpha$  con la condición  $0 \leqslant \alpha \leqslant 1$ , puede obtenerse del modo siguiente: escribimos las fracciones  $\frac{0}{1}$ ,  $\frac{1}{1}$ . Si  $2 \leqslant \tau$ , entonces entre estas

fracciones introducimos también la fracción  $\frac{0+1}{1+1} = \frac{1}{2}$ ,

después, en la sucesión obtenida  $\frac{0}{1}$ ,  $\frac{1}{2}$ ,  $\frac{1}{1}$  entre cada dos fracciones consecutivas  $\frac{a_1}{b_1}$  y  $\frac{c_1}{d_1}$  con  $b_1+d_1\leqslant \tau$  introducimos la fracción  $\frac{a_1+c_1}{b_1+d_2}$ , etc. y así continuamos siempre que esto sea posible. Demostrar previamente que para cualquier par de fracciones consecutivas  $\frac{a}{b}$  y  $\frac{c}{d}$  de la sucesión obtenida de este modo, se tiene ad-bc=-1.

b. Considerando la sucesión de Farey, demostrar el teorema: sea ₹ > 1, entonces cualquier número real α se puede expresar en la forma

$$\alpha = \frac{P}{Q} + \frac{\theta}{Q\tau}; \quad 0 < Q \leqslant \tau, \quad (P, Q) = 1, \quad |\theta| < 1.$$

- c. Demostrar el teorema de la pregunta b, aplicando g, § 4. 5, a. Demostrar que hay una cantidad infinita de números
- primos de la forma 4m + 3. **b.** Demostrar que hay una cantidad infinita de números primos de la forma 6m + 5.
- 6. Demostrar que la cantidad de números primos es infinita, calculando para ello la cantidad de números, no superiores a N, en cuyas descomposiciones canónicas no figuran números primos distintos de  $p_1, p_2, \ldots, p_k$ .
- 7. Sea K un número entero positivo. Demostrar que en la sucesión de números naturales hay un conjunto infinito de sucesiones M, M+1, ..., M+K-1, que no contienen números primos.
- 8. Demostrar que entre los números representados por el polinomio  $a_0x^n + a_1x^{n-1} + \ldots + a_n$ , donde n > 0,  $a_0$ ,  $a_1$ , ...,  $a_n$  son enteros y  $a_0 > 0$ , hay un conjunto infinito de números compuestos.
- 9, a. Demostrar que a la ecuación indeterminada

$$x^4 + y^3 = z^4$$
,  $x > 0$ ,  $y > 0$ ,  $z > 0$ ,  $(x, y, z) = 1$  (1) satisfacen aquellos sistemas  $x, y, z$ , y sólo aquéllos, en los

que uno de los números x e u tiene la forma 2uv, el otro tiene la forma  $u^a - v^a$  y, finalmente, z tiene la forma  $u^a + v^a$ ; en este caso u > v > 0, (u, v) = 1, uv es par.

b. Aplicando el teorema de la pregunta a, demostrar que la ecuación  $x^4 + y^4 = z^3$  es irresoluble en enteros positivos

X. U. Z.

10. Demostrar el teorema: si la ecuación  $x^n + a_1x^{n-1} +$  $+ \ldots + a_n = 0$ , donde n > 0 y  $a_i$ , . ,  $a_n$  son enteros, tiene una raíz racional, esta raíz es un número entero.

11, a. Sea  $S = \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$ ; n > 1. Demostrar que S no es entero.

**b.** Sea  $S = \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{2n+1}$ ; n > 0. Demostrar que S no es entero.

12. Sea n entero, n > 0. Demostrar que todos los coeficientes del desarrollo del binomio de Newton  $(a + b)^n$  son impares cuando, y sólo cuando, n tiene la forma  $2^h - 1$ .

#### Elercicios numéricos referentes al capitulo I

- 1, a. Aplicando el algoritmo de Euclides, hallar (6 188, 4 709).
- b. Hatlar (81 719, 52 003, 33 649, 30 107).
- 2, a. Desarrollando el número  $\alpha = \frac{125}{92}$  en fracción continua y formando la tabla de fracciones reducidas (d, § 4), hallar, α) δ,, β) la expresión de a en la forma indicada en la pregunta 4, b, considerando  $\tau = 20$
- b. Desarrollando  $\alpha = \frac{5391}{3076}$  en fracción continua y formando la tabla de fracciones reducidas, hallar α) δα, β) la expresión de α en la forma indicada en la pregunta 4, 5, considerando  $\tau = 1$  000.
- 8. Formar la sucesión de fracciones de Farey (pregunta 4) desde 0 hasta 1, excluyendo I, con los denominadores no superiores a 8
- 4. Formar la tabla de números primos menores de 100
- 5, a. Hallar la descomposición canónica del número 82 798 846
- b. Hallar la descomposición canónica del número 81 057 226 635 000

#### CAPITULO SEGUNDO

#### Las funciones más importantes de la teoría de los números

§ 1. Functiones a. En la teoría de los números desempeña [x],  $\{x\}$  un papel importante la función  $\{x\}$ ; ésta se define para todos los valores reales de x y representa el entero mayor, no superior a x. Esta función se llama parte entera de x.

Ejemplos.

$$[7] - 7; [2,6] = 2; [-4,75] 5.$$

A veces se considera también la función  $\{x\}$   $x = \{x\}$ . Esta función se llama parte fraccionaria de x. Ejemplos.

$$\{7\} = 0$$
,  $\{2,6\} = 0.6$ ;  $\{-4.75\} = 0.25$ .

 b. Para mostrar la utilidad de las funciones introducidas demostremos el teorema;

El exponente, con el que un número primo dado p figura en el producto n1, es igual a

$$\left[\frac{n}{\rho}\right] + \left[\frac{n}{\rho^2}\right] + \left[\frac{n}{\rho^2}\right] + \dots$$

En efecto, el número de factores en el producto nl que son múltiplos de  $\rho$ , es igual a  $\left[\frac{n}{\rho}\right]$ , entre ellos, múltiplos de  $\rho^2$  hay  $\left[\frac{n}{\rho^2}\right]$ ; entre estos últimos, múltiplos de  $\rho^3$  hay

 $\left\lceil \frac{n}{p^4} \right\rceil$ , etc. La suma de los números indicados da precisamente el exponente buscado, puesto que cada factor en el producto nl que sea múltiplo de  $p^m$ , pero no de  $p^{m+1}$ , se cuenta del modo indicado m veces, como múltiplo de p,  $p^2$ ,  $p^3$ , ..., y, finalmente, de  $p^m$ .

Ejemplo, El exponente con el que el múmero 3 figura en el producto 401 es igual a

$$\left[\frac{40}{3}\right] + \left[\frac{40}{9}\right] + \left[\frac{40}{27}\right] = 13 + 4 + 1 = 18$$

8 2. Sumas
extendidas
a los dioisores
de un número

a. En la teoría de los números desempenan un papel particularmente importante
las funciones multiplicativas. Una función θ (a) se llama multiplicativa, si se
cumplen las condiciones siguientes:

 La función θ (a) está definida para todos los enteros positivos a u no se anula para ningún a de éslos

2. Para cualesquiera positivos  $a_1$  y  $a_2$ , primos entre st, se liene

$$\theta (a_1a_2) := \theta (a_1) \theta (a_2).$$

**Ejemplo.** Fácilmente se observa que es multiplicativa la función  $\theta$  (a)  $\approx a^s$ , donde s es un número real o complejo arbitrario.

b. De las propiedades indicadas de la función  $\theta$  (a) se deduce, en particular, que  $\theta$  (1) = 1. En efecto, supongamos que  $\theta$  (a<sub>0</sub>) no es igual a cero, entonces  $\theta$  (a<sub>0</sub>) =  $\theta$  (1·a<sub>0</sub>) =  $\theta$  (1)  $\theta$  (a<sub>0</sub>), es decir,  $\theta$  (1) = 1. Además, resulta la siguiente propiedad importante: si  $\theta_1$  (a) y  $\theta_2$  (a) son funciones multiplicativas, entonces  $\theta_0$  (a) =  $\theta_1$  (a)  $\theta_2$  (a) también es una función multiplicativa. En efecto, se tiene

$$\theta_0(1) = \theta_1(1) \theta_2(1) = 1$$

Además, para 
$$(a_1, a_2) = 1$$
, obtenemos  $\theta_0$   $(a_1a_2) = \theta_1$   $(a_1a_2) \theta_2$   $(a_1a_2) = \theta_1$   $(a_1) \theta_1$   $(a_2) \theta_2$   $(a_3) \theta_2$   $(a_2) = \theta_1$   $(a_1) \theta_2$   $(a_1) \theta_2$   $(a_2) \theta_2$   $(a_2) \theta_3$   $(a_3) \theta_4$   $(a_3) \theta_6$   $(a_3)$ .

c. Sea  $\theta$  (a) una función multiplicativa y sea  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots$  $\dots p_k^{\alpha_k}$  la descomposición canónica del número a. Designando con la notación  $\sum_{d > a}$  la suma, extendida a todos los divisores d del número a, se tiene

$$\sum_{d \setminus a} \theta(d) = (1 + \theta(\rho_1) + \theta(\rho_1^a) + \ldots + \theta(\rho_1^{\alpha_1})) \ldots$$

$$\ldots (1+\theta(\rho_k)+\theta(\rho_k^2)+\ldots+\theta(\rho_k^{\alpha_k}))$$

(en el caso a — I se supone que el segundo miembro es igual a 1).

Para demostrar esta identidad, abramos los parêntesis en el segundo miembro. Se obtiene una suma de términos de la forma.

$$\begin{aligned} \theta \left( \rho_1^{\beta_1} \right) \theta \left( \rho_2^{\beta_2} \right) & \dots \theta \left( \rho_k^{\beta_k} \right) = \theta \left( \rho_1^{\beta_1} \rho_2^{\beta_2} & \dots \rho_k^{\beta_k} \right); \\ 0 \leqslant \beta_1 \leqslant \alpha_1, \ 0 \leqslant \beta_2 \leqslant \alpha_2, \ \dots, \ 0 \leqslant \beta_k \leqslant \alpha_{k_1} \end{aligned}$$

donde ninguno de tales términos se omite y no se repite más de una vez; esto es (e, § 6, cap. l), precisamente, lo que figura en el primer miembro.

d. Para  $\theta$  (a) = a' la identidad c toma la forma

$$\sum_{d \sim a} d' = (1 + p_1^a + p_1^{2a} + \dots + p_1^{\alpha_1 a}) ... (1 + p_2^a + p_2^{2a} + \dots + p_n^{\alpha_n a}).$$
(1)

En particular, para s 1 el primer miembro de (1) representa la suma de los divisores S (a) del número a. Simplificando el segundo miembro, obtenemos:

$$S(a) = \frac{\rho_1^{\alpha_1+1} - 1}{\rho_1 - 1} \cdot \frac{\rho_2^{\alpha_2+1} - 1}{\rho_2 - 1} = \frac{\rho_k^{\alpha_k+1} - 1}{\rho_k - 1}.$$

Ejemplo.

$$S(720) = S(2^4 \ 3^2 \cdot 5) = \frac{2^{4+1}-1}{2-1} \cdot \frac{3^{4+1}-1}{3-1} \cdot \frac{5^{i+1}-1}{5-1} = 2418.$$

Para s = 0 el primer miembro de (1) representa el número de divisores  $\tau$  (a) del número a, y se tiene:

$$\tau(a) = (a_1 + 1)(a_2 + 1) \dots (a_k + 1).$$

Ejemplo.

$$\tau$$
 (720) = (4 + 1) (2 + 1) (1 + 1) = 30.

§ 3. Fanción a. La función de Möbius  $\mu$  (a) se define de Möbius para todos los enteros positivos a. Esta se determina por las igualdades:  $\mu$  (a) = 0 si a es divisible por un cuadrado distinto de la unidad;  $\mu$  (a) =  $(-1)^k$ , si a no es divisible por un cuadrado distinto de la unidad, donde k denota el número de divisores primos del número a, en particular, para a=1 se considera k=0, por lo cual admitimos que  $\mu$  (1) = 1.

Ejempios.

$$\mu(1) = 1,$$
  $\mu(5) = -1,$   $\mu(9) = 0,$   
 $\mu(2) = -1,$   $\mu(6) = 1,$   $\mu(10) = 1,$   
 $\mu(3) = -1,$   $\mu(7) = -1,$   $\mu(11) = -1,$   
 $\mu(4) = 0,$   $\mu(8) = 0,$   $\mu(12) = 0.$ 

b. Sea θ (a) una función multiplicativa y sea

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

la descomposición canónica del número a. Entonces

$$\sum_{\mathbf{d} \subseteq \mathbf{d}} \mu(\mathbf{d}) \, \theta(\mathbf{d}) = (1 - \theta(p_1)) \, (1 - \theta(p_2)) \, \dots \, (1 - \theta(p_k)).$$

(En el caso a = 1 se supone que el segundo miembro es igual a 1).

En efecto, la función  $\mu$  (a), evidentemente, es multiplicativa. Por esto, es multiplicativa también la función  $\theta_1$  (a) =  $\mu$  (a)  $\theta$  (a). Aplicando a esta última la identidad c, § 2

y teniendo en cuenta que  $\theta_1(p) = -\theta(p)$ ;  $\theta_1(p^*) = 0$  para s > 1, nos convencemos de que el teorema es justo.

c. En particular, haciendo  $\theta$  (a) = 1, de b obtenemos

$$\sum_{\mathbf{d} \setminus a} \mu (\mathbf{d}) = \begin{cases} 0, & \text{si } a > 1, \\ 1, & \text{si } a = 1. \end{cases}$$

Haciendo  $\theta(d) = \frac{1}{d}$ , resulta

$$\sum_{d \searrow a} \frac{\mu(d)}{d} - \left\{ \begin{pmatrix} 1 - \frac{1}{\rho_1} \end{pmatrix} \left( 1 - \frac{1}{\rho_2} \right), & (1 - \frac{1}{\rho_2}), & \text{si } a > 1, \\ 1, & \text{si } a = 1. \end{pmatrix}$$

d. Supongamos que a los enteros positivos

$$\delta = \delta_1, \delta_2, \ldots, \delta_n$$

les corresponden cualesquiera valores reales o complejos  $f=f_1,\ f_2,\dots,f_n$  Entonces, designando con la notación S' la suma de los valores f que corresponden a los valores iguales a f, g con la notación  $S_d$  la suma de los valores f que corresponden a los valores f que son múltiplos de f, se tiene

$$S' = \sum \mu(d) S_d,$$

donde d recorre todos los números enteros positivos que dividen al menos un valor 8.

En efecto, en virtud de c, se tiene

$$S' = f_1 \sum_{d > \delta_1} \mu(d) + f_2 \sum_{d > \delta_2} \mu(d) + \dots + f_n \sum_{d > \delta_n} \mu(d).$$

Reuniendo todos los términos con un mismo valor de d y sacando luera de paréntesis  $\mu$  (d), obtendremos entre paréntesis la suma de aquellos números f, y sólo aquéllos, cuyos  $\delta$  correspondientes son múltiplos de d, y esto es precisamente  $S_d$ 

§ 4. Panción a. La función de Euler  $\varphi$  (a) se define para todos los enteros positivos a y representa la cantidad de números de la sucesión

$$0, 1, \ldots, a-1$$
 (1)

que son primos con a.

Ejemplos.

$$\varphi(1) = 1, \quad \varphi(4) = 2,$$
  
 $\varphi(2) = 1, \quad \varphi(5) = 4,$   
 $\varphi(3) = 2, \quad \varphi(6) = 2.$ 

b. Sea

$$a = \rho_1^{\alpha_1} \rho_2^{\alpha_2} \dots \rho_k^{\alpha_k} \tag{2}$$

la descomposición canónica del número a. Entonces

$$\varphi(a) = a \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right),$$
 (3)

o también

$$\Psi(a) = (\rho_1^{\alpha_1} - \rho_1^{\alpha_1-1}) (\rho_2^{\alpha_2} - \rho_2^{\alpha_2-1}) . . (\rho_k^{\alpha_k} - \rho_k^{\alpha_k-1}); \quad (4)$$

en particular,

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}, \quad \varphi(p) = p - 1.$$
 (5)

En efecto, apliquemos el teorema d, § 3. En este caso, los números  $\delta_h$  y los números  $f_h$  los definimos así: Supongamos que k recorre los números de la sucesión (1). Hagamos  $\delta_h = (k, a)$  y a cada valor  $\delta_h$  le ponemos en correspondencia el número  $f_h = 1$ .

Entonces S' será igual al número de valores de  $\delta_k = (k, a)$  que son iguales a 1, es decir, será igual a  $\varphi(a)$ , mientras que  $S_d$  será igual al número de valores de  $\delta_k = (k, a)$  que son múltiplos de d. Pero (k, a) puede ser múltiplo de d solamente bajo la condición de que d sea un divisor de a Cumpliéndose esta condición,  $S_d$  será igual al número de valores de k que son múltiplos de d, es decir, será igual a  $\frac{a}{d}$  Así, pues, resulta

$$\varphi(a) = \sum_{d \geq a} \mu(d) \frac{a}{d}$$

de donde, en virtud de c, § 3, se deduce la fórmula (3), y de esta última, en virtud de (2), se deduce la fórmula (4).

Elemplos.

$$\varphi(60) = 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{6}\right) = 16;$$
  
 $\varphi(81) = 81 - 27 = 54;$   
 $\varphi(5) = 5 - 1 = 4.$ 

c. La función φ (a) es multiplicativa.

En efecto, para  $(a_1, a_2) = 1$  de b, evidentemente, se deduce que

$$\varphi (a_1 a_2) = \varphi (a_1) \varphi (a_2).$$
  
Ejempto.  $\varphi (405) = \varphi (81) \varphi (5) = 54.4 = 216$   
d.  $\sum_{d > a} \varphi (d) = a.$ 

Para verificar esta fórmula, aplicamos la identidad c, § 2, la cual para  $\theta$  (a) =  $\varphi$  (a) da

$$\sum_{d = 0}^{\infty} \varphi(d) = (1 + \varphi(\rho_1) + \varphi(\rho_1^a) + \ldots + \varphi(\rho_1^{a_1})) \ldots$$
$$\ldots (1 + \varphi(\rho_k) + \varphi(\rho_k^a) + \ldots + \varphi(\rho_k^{a_k}))$$

En virtud de (5) el segundo miembro se escribe así-

$$(1+(p_1-1)+(p_1^2-p_1)+\ldots+(p_1^{\alpha_1}-p_1^{\alpha_1-1}))\ldots (1+(p_k-1)+(p_k^2-p_k)+\ldots+(p_k^{\alpha_k}-p_k^{\alpha_k-1})).$$

lo cual, después de reducir los términos semejantes en cada paréntesis grande, resulta ser igual a  $p_k^{\alpha_1}$   $p_k^{\alpha_2}$  .  $p_k^{\alpha_k} = a$  Ejempio. Haciendo a = 12, hallamos

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) =$$
= 1 + 1 + 2 + 2 + 2 + 4 = 12

#### Preguntas referentes al capitalo !!

1, a. Supongamos que en el intervalo  $Q \le x \le R$  la función f(x) es continua y no negativa. Demostrar que la suma

$$\sum_{Q$$

expresa el número de puntos enteros (puntos de coordenadas enteras) de la región plana:  $Q < x \le R$ ,  $0 < y \le f(x)$ . b. Sean P y Q números positivos impares, primos entre sí. Demostrar que

$$\sum_{0 < x < \frac{Q}{2}} \left[ \left. \frac{P}{Q} x \right] + \sum_{0 < y < \frac{P}{2}} \left[ \left. \frac{Q}{P} y \right] = \frac{P-1}{2} \cdot \frac{Q-1}{2} \right.$$

c. Supongamos que r>0 y sea T el número de puntos enteros que hay en la región  $x^2 + y^2 \le r^2$ . Demostrar que

$$T = 1 + 4[r] + 8 \sum_{0 < x \le \frac{r}{\sqrt{2}}} \left[ \sqrt{r^2 - x^2} \right] - 4 \left[ \frac{r}{\sqrt{2}} \right]^2$$

d. Supongamos que n>0 y sea T el número de puntos enteros que hay en la región x>0, y>0, xy < n. Demostract que

$$T = 2 \sum_{0 < x \leq \sqrt[n]{n}} \left\lceil \frac{n}{x} \right\rceil - [\sqrt[n]{n}]^2.$$

e. Consideremos un polígono, cuyos vértices son puntos enteros y cuyo contorno no se corta consigo mismo y no es tangente a sí mismo. Sea S el área del polígono y  $T = \sum \delta - 1$ , donde la sumación se extiende a todos los puntos enteros que están situados en el interior del polígono y en su contorno, siendo  $\delta=1$  para los puntos interiores y  $\delta=0.5$  para los puntos del contorno. Demostrar que T = S.

2. Supongamos que n > 0, m es entero, m > 1 y x recorre los números enteros positivos que no son divisibles por la m-ésima potencia de un entero superior a 1. Demostrar que

$$\sum_{n} \left[ \sqrt[n]{\frac{n}{x}} \right] = [n].$$

 Supongamos que los números positivos α y β son tales que

$$[\alpha x]; x = 1, 2, \ldots; [\beta y]; y = 1, 2, \ldots$$

forman conjuntamente todos los números de la sucesión natural sin repeticiones. Demostrar que esto se cumple cuando, y sólo cuando, a es irracional y

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1.$$

**4.** a. Sea  $[\tau] \ge 1$ ,  $t = [\tau]$  y sean  $x_1, x_2, \dots, x_t$  los números 1, 2, ... I, dispuestos en tal orden que los números

$$0, \{\alpha x_1\}, \{\alpha x_2\}, \ldots, \{\alpha x_t\}, 1$$

no decrezcan. Demostrar el teorema de la pregunta 4, b, cap. 1. considerando las diferencias de los números consecutivos de la última sucesión

b. Sean  $\tau_1, \ \tau_2, \ \dots, \ \tau_k$  números reales, cada uno de los cuales no es menor que 1; supongamos que  $\alpha_1, \alpha_2, \ldots, \alpha_k$ son reales. Demostrar que existen unos números enteros ξ<sub>1</sub>, ξ<sub>2</sub>, . . . , ξ<sub>k</sub>, no simultáneamente iguales a cero, y un número entero n, que satisfacen a las condiciones:

$$\begin{split} |\xi_1| \leqslant & \tau_1, \ |\xi_2| \leqslant \tau_2, \dots, |\xi_k| \leqslant & \tau_k, (\xi_1, \xi_2, \dots, \xi_k, \eta) = 1, \\ |\alpha_1 \xi_1 + \alpha_2 \xi_2 + \dots + \alpha_k \xi_k + \eta| \leqslant \frac{1}{\tau_1 \tau_k}. \end{split}$$

5. Sea  $\alpha$  real y c entero, c > 0. Demostrar que

$$\left[ \frac{[\alpha]}{c} \right] = \left[ \frac{\alpha}{c} \right].$$

6. a. Sean α. β. ... λ números reales Demostrar que  $[\alpha + \beta + + \lambda] \geqslant [\alpha] + [\beta] + + + [\lambda].$ 

b. Supongamos que a, b, . , l son enteros positivos. a + b + . + l = n. Aplicando b, § 1, demostrar que

es un número entero.

7. Supongamos que h es entero, h > 0, p es primo y

$$u_k = \frac{p^{a+1}-1}{p-1}.$$

Representando h en la forma  $h=p_mu_m+p_{m-1}u_{m-1}+\dots+p_1u_1+p_0$ , donde  $u_m$  es el máximo  $u_a$  no superior a h,  $p_mu_m$  es el máximo múltiplo de  $u_m$  no superior a h,  $p_{m-1}u_{m-1}$  es el máximo múltiplo de  $u_{m-1}$  no superior a h —  $-p_mu_m, p_{m-2}u_{m-2}$  es el máximo múltiplo de  $u_{m-1}$  no superior a h —  $p_mu_m, p_{m-2}u_{m-2}$  es el máximo múltiplo de  $u_{m-2}$  no superior a h —  $p_mu_m - p_{m-1}u_{m-1}$ , etc, demostrar que los números a que satisfacen a la condición de que en la descomposición canónica de a! el número p figura con el exponente h, existen cuando, p sólo cuando, todos los números  $p_m$ ,  $p_{m-1}, \dots, p_1, p_0$  son menores que p; además, en este caso los números a indicados son todos los de la forma

$$a = p_m p^{m+1} + p_{m-1} p^m + \dots + p_1 p^3 + p_0 p + p^*$$

donde p' toma los valores:  $0, 1, \ldots, p-1$ . 8, a. Supongamos que en el intervalo  $Q \leqslant x \leqslant R$  la función f(x) admite derivada segunda continua. Haciendo

$$\rho\left(x\right) = \frac{1}{2} - \left\{x\right\}, \quad \sigma\left(x\right) = \int_{0}^{x} \rho\left(z\right) dz,$$

demostrar que (fórmula de Sonin)

$$\sum_{Q<\alpha\leq R} f(x) = \int_{Q}^{\pi} f(x) dx + \rho(R) f(R) - \rho(Q) f(Q) - \sigma(R) f'(R) + \sigma(Q) f'(Q) + \int_{Q}^{\pi} \sigma(x) f''(x) dx.$$

Supongamos que se cumple la condición de la pregunta
 para R arbitrariamente grandes, y que la integrat

 $\int_{0}^{\infty} |f''(x)| dx \text{ es convergente. Demostrar que}$ 

$$\sum_{Q < x \le R} f(x) =$$

$$= C + \int_{R}^{R} f(x) dx + \rho(R) f(R) - \sigma(R) f'(R) - \int_{0}^{\infty} \sigma(x) f''(x) dx$$

donde C no depende de R.

c. Si B toma solamente valores positivos y la razón  $\frac{|A|}{B}$  permanece acotada superiormente, se escribe A = O(B). Sea n entero, n > 1. Demostrar que

$$\ln (n1) = n \ln n - n + O(\ln n).$$

**0**, **a.** Sea  $n \ge 2$ ,  $\Theta(z, z_0) = \sum_{z_0 , donde <math>p$  recorre los números primos. Sea también  $\Theta(z) = \Theta(z, 0)$  y para x > 0

$$\psi(x) = \Theta(x) + \Theta(\sqrt{x}) + \Theta(\sqrt[3]{x}) + \dots$$

Demostrar que

$$\alpha) \quad \ln\left([n]!\right) = \psi\left(n\right) + \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) + \cdots$$

$$\beta$$
)  $\psi(n) < 2n$ ;

$$\gamma) \quad \Theta\left(n, \frac{n}{2}\right) + \Theta\left(\frac{n}{3}, \frac{n}{4}\right) + \Theta\left(\frac{n}{5}, \frac{n}{6}\right) + \dots = \\ = n \ln 2 + O\left(\sqrt{n}\right).$$

**b.** Para n > 2, demostrar que

$$\sum_{n\leq n}\frac{\ln p}{p}=\ln n+O(1).$$

donde p recorre números primos.

c. Sea e una constante positiva arbitraria. Demostrar que en la sucesión de números naturales existe un conjunto infinito de pares de números primos  $p_n$ ,  $p_{n+1}$  que satisfacen a la condición

$$\rho_{n+i} < \rho_n \ (1+\varepsilon).$$

**d.** Sea n > 2. Demostrar que

$$\sum_{n \le n} \frac{1}{\rho} = C + \ln \ln n + O\left(\frac{1}{\ln n}\right),$$

donde p recorre números primos y C no depende de n. e. Sea n > 2. Demostrar que

$$\prod_{n \le n} \left( 1 - \frac{1}{\rho} \right) = \frac{C_0}{\ln n} \left( 1 + O\left( \frac{1}{\ln n} \right) \right),$$

donde p recorre números primos y  $C_0$  no depende de n.

f. Demostrar la existencia de una constante  $s_0 > 2$  con la condición de que para cualquier entero  $s > s_0$ , para el s-ésimo número primo  $p_s$  de la aucesión 2, 3, 5, . . . se verifica la desigualdad

$$p_a < 1.58 \text{ ln s}.$$

g. Demostrar que

$$\frac{a}{w(a)} = O(\ln \ln a).$$

10. a. Sea  $\theta$  (a) una función multiplicativa. Demostrar que  $\theta_1$  (a) =  $\sum_{i=1}^{n} \theta_i(d)$  también es una función multiplicativa.

b. Supongamos que la función  $\theta(a)$  está definida para todos los enteros positivos a y que la función  $\psi(a) \cdot \sum_{d \in a} \theta(a)$  es multiplicativa. Demostrar que la función  $\theta(a)$  también es multiplicativa.

11. Supongamos que, para m > 0,  $\tau_m$  (a) denota el número de soluciones de la ecuación indeterminada  $x_1x_2 \ldots x_m = a(x_1, x_2, \ldots, x_m \text{ recorren los números enteros positivos})$ 

independientemente uno de otro); en particular, es evidente que  $\tau_1$  (a) = 1,  $\tau_2$  (a) =  $\tau$  (a) Demostrar que

a. τ<sub>m</sub> (a) es una función multiplicativa.

b. Sea p un número primo,  $\alpha \ge 0$  y m > 1. Entonces

$$\tau_m(p^{\alpha}) = \frac{(\alpha+1)(\alpha+2)\ldots(\alpha+m-1)}{1\cdot 2\ldots(m-1)}.$$

c. Si e es una constante positiva arbitraria, se tiene

$$\lim_{a\to\infty}\frac{\tau_m(a)}{a^a}=0.$$

d.  $\sum_{0 < n \le n} \tau_m(a)$  express el número de soluciones de la desigualdad  $x_1 x_2 \ldots x_m \le n$  en números enteros positivos  $x_i$ ,  $x_2, \ldots, x_m$ .

 Supongamos que R (s) representa la parte real del número s.

Si R(s) > 1, hacemos  $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ . Sea m > 0, m es

entero. Demostrar que

$$(\zeta(s))^m = \sum_{m=1}^{\infty} \frac{\tau_m(n)}{n!}.$$

13, a. Siendo R(s) > 1, demostrar que

$$\zeta(s) = \prod \frac{1}{1 - \frac{1}{\rho^s}},$$

donde p recorre todos los números primos.

 b. Demostrar que la cantidad de números primos es infinita, hasándose en la divergencia de la serie armónica.

c. Demostrar que la cantidad de números primos es infinita, basándose en la irracionalidad del número  $\zeta(2) = \frac{\pi^3}{\pi}$ .

14. Sea  $\Lambda(a) = \ln p$  para  $a = p^t$ , donde p es primo y l es un entero positivo;  $\Lambda(a) = 0$  para los otros enteros posi-

tivos a. Siendo R (s) > 1, demostrar que

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}.$$

15. Sea R(s) > 1 Demostrar que

$$\prod_{n=1}^{\infty} \left(1 - \frac{1}{p^{\alpha}}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}}.$$

donde p recorre los números primos.

16, a. Sea n ≥ 1. Aplicando d, § 3, demostrar que

$$l = \sum_{0 < d \leqslant n} \mu(d) \left\lceil \frac{n}{d} \right\rceil.$$

b. Sea  $M(z, z_0) = \sum_{z_0 < a \leqslant z} \mu(a); \quad M(x) = M(x, 0).$  Demostrar que

$$\alpha) \ M(n) + M\left(\frac{n}{2}\right) + M\left(\frac{n}{3}\right) + \ldots = 1, \ n \gg 1.$$

$$\beta) M\left(n, \frac{n}{2}\right) + M\left(\frac{n}{3}, \frac{n}{4}\right) + M\left(\frac{n}{5}, \frac{n}{6}\right) + \dots = -1, n > 2.$$

c. Supongamos que  $n \ge 1$ , l es entero, l > 1,  $T_{l,n}$  es el número de enteros x con la condición  $0 < x \le n$ , que no son divisibles por la l-ésima potencia de un entero superior a l. Aplicando d, § 3, demostrar que

$$T_{t,n} = \sum_{d=1}^{n} \mu(d) \left[ \frac{n}{d^{t}} \right].$$

17, a. Supongamos que a es entero, a>0, y que para los enteros  $x_1, x_2, \dots, x_n$  se ha definido univocamente una función f(x). Demostrar que

$$S' = \sum_{n} \mu(d) S_d$$

donde S' denota la suma de los valores de f(x), extendida a los valores de x que son primos con a, y  $S_d$  es la suma de

los valores de f(x), extendida a los valores de x que son múltiplos de d.

b. Supongamos que k > 1 y que se han dado los sistemas

$$x_1', x_2', \ldots, x_k', x_1', x_2', \ldots, x_k^n; \ldots; x_1^{(n)}, x_2^{(n)}, \ldots, x_k^{(n)},$$

donde cada uno de ellos consta de números enteros no simultáneamente iguales a cero. Supongamos también que para estos sistemas se ha definido univocamente una función  $f(x_1, x_2, \ldots, x_h)$ . Demostrar que

$$S' := \sum \mu(d) S_d$$

donde S' denota la suma de los valores de  $f(x_1, x_2, \ldots, x_h)$ , extendida a los sistemas de números primos entre sí, y  $S_d$  es la suma de los valores de  $f(x_1, x_2, \ldots, x_h)$ , extendida a los sistemas de números que son simultáneamente múltiplos de d. Aquí d recorre números enteros positivos.

c. Supongamos que a es entero, a > 0, y que para los divisores  $\delta$  del número a se ha definido univocamente una función  $F(\delta)$ . Haciendo

$$G(\delta) = \sum_{d > \delta} F(d),$$

demostrar que (la ley de inversión para las funciones numéricas)

$$F(a) = \sum_{d \geq a} \mu(d) G\left(\frac{a}{d}\right)$$

d. Supongamos que a los enteros positivos

$$\delta_1, \ \delta_2, \ \ldots, \ \delta_n$$

les corresponden cualesquiera números reales o complejos, no iguales a cero:

Demostrar que

$$P' = \prod P_d^{\mu(d)},$$

donde P' denota el producto de los valores f que corresponden a los valores  $\delta$  que son iguales a 1,  $P_d$  denota el producto

de los valores f que corresponden a los valores  $\delta$  que son múltiplos de d, y d recorre todos los números enteros positivos que dividen al menos a un  $\delta$ .

- 18. Supongamos que a es entero, a > 1,  $\sigma_m(n) = 1^m + 2^m + \ldots + n^m$ ,  $\psi_m(a)$  es la suma de las m-ésimas potencias de los números de la sucesión  $1, 2, \ldots, a$  que son primos con a;  $p_1, p_2, \ldots, p_k$  son los divisores primos del número a.
- Aplicando el teorema de la pregunta 17, a, demostrar que

$$\psi_{m}\left(a\right) = \sum_{d \searrow a} \mu\left(d\right) d^{m} \sigma_{m}\left(\frac{a}{d}\right).$$

b. Demostrar que

$$\psi_1(a) = \frac{a}{2} \, \psi(a)$$
.

c. Demostrar que

$$\psi_{8}(a) = \left(\frac{a^{2}}{3} + \frac{(-1)^{h}}{6} \rho_{1} p_{2} \dots p_{h}\right) \varphi(a).$$

- 19. Supongamos que z > 1, a es entero, a > 0,  $T_z$  es la cantidad de números x con las condiciones  $0 < x \le z$ , (x, a) = 1, z es una constante positiva arbitraria.
- a. Demostrar que

$$T_{z} = \sum_{d > a} \mu(d) \left[ \frac{z}{d} \right].$$

b. Demostrar que

$$T_z = \frac{z}{a} \varphi(a) + O(a^a).$$

c. Supongamos que z > 1,  $\pi$  (z) denota la cantidad de números primos no superiores a z, a es el producto de los números primos no superiores a  $\sqrt{z}$ . Demostrar que

$$\pi(z) - \pi(\sqrt{z}) - 1 + \sum_{d > a} \mu(d) \left[\frac{z}{d}\right].$$

20. Supongamos R(s) > 1, a es entero, a > 0. Demostrar que

 $\sum\nolimits{'}\frac{1}{n^{s}} = \zeta \ (s) \ \prod \ \left(1 - \frac{1}{n^{s}}\right),$ 

donde n recorre en el primer miembro los números enteros positivos que son primos con a, y p recorre en el segundo miembro todos los divisores primos del número a.

- 21, a. La probabilidad P de que k números enteros positivos  $x_1, x_2, \ldots, x_k$  sean primos entre si, la definiremos como el limite para  $N \to \infty$  de la probabilidad  $P_N$  de que sean primos entre si k números  $x_1, x_2, \ldots x_k$ , a cada uno de los cuales, independientemente de los demás, se le ha asignado uno de los valores 1, 2, ..., N, los cuales se consideran como valores igualmente posibles. Aplicando el teorema de la pregunta 17, b, demostrar que  $P = (\zeta(k))^{-1}$ .
- b. Definiendo la probabilidad P de que la fracción  $\frac{x}{y}$  sea irreducible del mismo modo que en la pregunta a para k=2, demostrar que

 $P = \frac{8}{n^2}$ .

22, a. Supongamos que  $r \ge 2$ , y sea T el número de puntos enteros (x, y) situados en la región  $x^2 + y^3 \le r^3$ , y cuyas coordenadas son números primos entre sí Demostrar que

$$T = \frac{6}{\pi} r^{\frac{\alpha}{4}} + O(r \ln r).$$

b. Supongamos que  $r \ge 2$ , y sea T el número de puntos enteros (x, y, z) situados en la región  $x^3 + y^3 + z^3 \le r^3$ , y cuyas coordenadas son números primos entre si. Demostrar que

$$T = \frac{4\pi}{3\xi(3)} r^3 + O(r^3).$$

23, a. Demostrar el teorema c, § 3, contando los divisores del número a que no son divisibles por el cuadrado de un entero superior a 1 y que tienen 1, 2, . . divisores primos.

- b. Supongamos que a es entero, a>1, d recorre los divisores del número a que tienen no más de m divisores primos. Demostrar que para m par,  $\sum \mu$   $(d) \geqslant 0$ , y para m impar,  $\sum \mu$   $(d) \leqslant 0$ .
- c. En las condiciones del teorema d, § 3, considerando que todos los valores f son no negativos y haciendo recorrer a d solamente los números que tienen no más de m divisores primos, demostrar que

$$S' \leqslant \sum \mu(d) S_d$$
,  $S' \geqslant \sum \mu(d) S_d$ 

según que m sea par o impar.

- d. En las condiciones de la pregunta 17, a, demostrar unas designaldades iguales a las de la pregunta c, considerando que todos los valores de f(x) son no negativos, hacer lo mismo también en las condiciones 17, b, considerando que todos los valores  $f(x_1, x_2, \ldots, x_k)$  son no negativos.
- 24. Supongamos que e es cualquier constante con las condiciones  $0 < \varepsilon < \frac{1}{6}$ ,  $N \ge 8$ ,  $r = \ln N$ ,  $0 < q \le N^{t-\epsilon}$ ,  $0 \le t < < q$ , (q, t) = 1,  $\pi(N, q, t)$  es la cantidad de números primos con las condiciones:  $p \le N$ , p = qt + t, donde t es entero. Demostrar que

$$\pi\left(N,\,q,\,l\right)=O\left(\Delta\right);\quad \Delta=\frac{Nr^{2}}{r\psi\left(q\right)}.$$

Para la demostración, haciendo  $h=r^{1-0,8e}$ , los números primos con las condiciones indicadas se deben considerar como un caso particular de todos los números con estas condiciones que son primos con a, donde a es el producto de todos los primos que no son superiores a  $e^h$  y que no dividen a q. Se debe aplicar el teorema de la pregunta 23, d (condiciones de la pregunta 17, a) con el a indicado y m=2(2 in r+1).

25. Supongamos que k es par, k > 0, la descomposición canónica del número a tiene la forma  $a = p_1p_2 \dots p_k$  y d recorre los divisores del número a con la condición

0 < d < Va Demostrar que

$$\sum \mu (d) = 0.$$

26. Supongamos que k es entero, k > 0, d recorre los números con la condición  $\varphi(d) = k$ . Demostrar que

$$\sum_{d}\mu\left( d\right) =0.$$

- 27. Utilizando la expresión de φ (a), demostrar que la cantidad de números primos es infinita
- 28, a. Demostrar el teorema d, § 4, estableciendo que la cantidad de números de la sucesión 1, 2, ..., a que tienen con a un mismo máximo común divisor  $\delta$ , es igual a  $\phi\left(\frac{a}{\delta}\right)$ .
- b. Deducir la expresión para φ (a):
- a) aplicando el teorema de la pregunta 10, b;
- β) aplicando el teorema de la pregunta 17, c
- 29. Sea R (s) > 2. Demostrar que

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^d} = \frac{\zeta(d-1)}{\zeta(s)}.$$

30. Sea n entero,  $n \gg 2$ . Demostrar que

$$\sum_{m=1}^{n} \varphi(m) = \frac{3}{n^2} n^3 + O(n \ln n).$$

### Ejercicios numéricos referentes al capitalo II

- 1, a. Hallar el exponente con el que el número 5 figura en la descomposición canónica de 5 2581 (yéase la pregunta 5).
- b. Hatlar la descomposición canónica del número 1251
- 2, a. Hallar v (5 600) y S (5 600).
- b. Hallar t (116 424) y S (116 424).
- 3. Formar la table de los valores de la función  $\mu$  (a) para todos los  $\alpha=1,\ 2,\ \dots$  100
- 4. Hallat α) φ (5 040), β) φ (1 294 700).
- 6 Formar la tabla de los valores de la función φ (a) para todos los a = 1 2, ..., 50, aplicando solamente la fórmula (5), § 4 y el teo rema c, § 4

## CAPITULO TERCERO

# Congruencias

§ 1. Conceptos a. Vamos a estudiar los números enteros fundamentales en relación con los restos de la división de los mismos por un entero positivo m dado, al cual lo liamaremos módulo.

A cada número entero le corresponde el resto de su división por m (c, § 1, cap. 1); si a dos enteros a y b les corresponde un mismo resto r, éstos se liaman congruentes según el módulo m, o respecto del módulo m, o simplemente, congruentes módulo m.

 b. La congruencia de los números a y b respecto del módulo m se escribe así:

$$a \Longrightarrow b \pmod{m}$$
.

lo cual se lee: a es congruente con b respecto del módulo m.

c. La congruencia de los números a y b respecto del módulo m es equivalente a:

1. La posibilidad de expresar a en la forma a = b + mt, donde t es entero.

La divisibilidad de a — b por m.

En efecto, de a = b (mód. m) se deduce que

$$a = mq + r$$
,  $b = mq_s + r$ ;  $0 \le r < m$ ,

de donde

$$a - b = m (q - q_i), a = b + ml, l = q - q_i.$$

Reciprocamente, de a = b + mt, representando b en la forma  $b = mq_1 + r$ ,  $0 \le r < m$ ,

deducimos que

$$a = mq + r; \quad q = q_1 + l.$$

es decir,

$$a = b \pmod{m}$$
.

Por esto, la afirmación 1 es justa.

De 1 se deduce inmediatamente la afirmación 2.

§ 2. Propiedades de las congruencias, semejantes a las propiedades de las igualdades a. Dos números que son congruentes con un tercero, son congruentes entre si.

Se deduce de a, § 1.

b. Las congruencias se pueden sumar término a término.

En efecto, sea

$$a_1 \equiv b_1 \pmod{m}, \quad a_2 \equiv b_2 \pmod{m}, \dots,$$

$$a_k = b_k \pmod{m}$$
. (1)

Entonces, (1, c, § 1),

$$a_1 = b_1 + mt_1$$
,  $a_2 = b_2 + mt_2$ , . .,  $a_k = b_k + mt_k$ , (2) de donde

$$a_1 + a_2 + \ldots + a_k = b_1 + b_2 + \ldots + b_k + m (t_1 + t_2 + \ldots + t_k),$$

o sea, (1, c, § 1),

$$a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod{m}$$
.

Un sumando que figure en un miembro cualquiera de la congruencia se puede pasar al otro miembro, cambiándole el signo.

En efecto, sumando la congruencia  $a+b\equiv c\pmod{m}$  con la congruencia evidente  $-b\equiv -b\pmod{m}$ , resulta  $a\equiv c-b\pmod{m}$ .

A cada miembro de una congruencia se le puede sumar (o restar) cualquier número que sea múltiplo del módulo.

En efecto, sumando la congruencia  $a \equiv b \pmod{m}$  con la congruencia evidente  $mk \equiv 0 \pmod{m}$ , resulta  $a + mk \equiv b \pmod{m}$ .

c. Las congruencias se pueden multiplicar término a término.

En efecto, examinemos de nuevo las congruencias (1) y las igualdades (2) que se deducen de ellas. Multiplicando término a término las igualdades (2), obtenemos

$$a_1a_1\ldots a_k=b_1b_1\ldots b_k+mN.$$

donde N es entero. Por consiguiente, (1, c, § 1).

$$a_1a_2 \dots a_k \equiv b_1b_2 \dots b_k \pmod{m}$$
.

Ambos miembros de la congruencia se pueden elevar a una misma potencia.

Esto se deduce del aserto anterior

Ambos miembros de la congruencia se pueden multiplicar por un mismo entero.

En efecto, multiplicando la congruencia  $a = b \pmod{m}$  por la congruencia evidente  $k = k \pmod{m}$ , obtenemos  $ak = bk \pmod{m}$ .

d. Las propiedades b y c (la adición y multiplicación de congruencias) se generalizan mediante el siguiente teorema Si en la expresión de una función racional entera de coeficientes enteros

$$S = \sum A_{\alpha_1, \ldots, \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k}$$

se sustituyen los números  $A_{\alpha_1,\ldots,\alpha_h}$ ,  $x_1,\ldots,x_h$  por los números  $B_{\alpha_1,\ldots,\alpha_h}$ ,  $y_1,\ldots,y_h$ , los cuales son congruentes con los anteriores respecto del módulo m, la expresión nueva de S será congruente con la precedente respecto del módulo m

En efecto, de

$$A_{n_1, \ldots, n_k} = B_{n_1, \ldots, n_k} \pmod{m}$$
  
 $x_1 = y_1 \pmod{m}, \qquad x_k = y_k \pmod{m}$ 

hallamos (c)

$$x_1^{\alpha_1} \equiv y_1^{\alpha_1} \pmod{m}, \quad , \quad x_k^{\alpha_k} \equiv y_k^{\alpha_k} \pmod{m}.$$

$$A_{\alpha_1, \ldots, \alpha_h} x_1^{\alpha_1} \ldots x_h^{\alpha_h} = B_{\alpha_1, \ldots, \alpha_h} y_1^{\alpha_1} \cdots y_h^{\alpha_h} \pmod{m}$$

de donde, sumando, obtenemos

$$\sum_{\alpha_k} A_{\alpha_1}, \quad x_k^{\alpha_1} = \sum_{\alpha_k} B_{\alpha_1}, \quad x_k^{\alpha_k} = \sum_{\alpha_k} B_{\alpha_1}, \quad x_k^{\alpha_k} = \sum_{\alpha_k} B_{\alpha_1}, \quad x_k^{\alpha_k} = \sum_{\alpha_k} B_{\alpha_1}$$

$$a \equiv b \pmod{m}, \quad a_1 \equiv b_1 \pmod{m}, \quad a_n = b_n \pmod{m},$$

$$x \equiv x_1 \pmod{m},$$

se liene

$$ax^{n} + a_{1}x^{n-1} + \dots + a_{n} = bx_{1}^{n} + b_{1}x_{1}^{n-1} + \dots + b_{n} \pmod{m}$$

Este aserto es un caso particular del anterior

e. Ambos miembros de la congruencia se pueden dividir por su común divisor, si este último es primo con el módulo

En efecto, s<sub>1</sub> a = b (mód. m),  $a = a_1d$ ,  $b = b_1d$ , (d, m) = 1resulta que la diferencia a = b, igual a  $(a_1 = b_1) d$ , es divisible por m Por esto (2, 1, § 2, cap 1)  $a_1 - b_1$  es divisible por  $m_1$  es decir,  $a_1 = b_1 \pmod{m}$ .

a. Ambos miembros de una congruencia § 3. Otras propiedades de y el módulo se pueden multiplicar par las congruencias un mismo número entero

En efecto, de  $u = b \pmod{m}$  se deduce que

$$a = b + ml$$
,  $ak = bk + mkt$ 

y, por consigniente,  $ak = bk \pmod{mk}$ 

b. Ambos miembros de una congruencia y el módulo se pueden dividir por cualquier común divisor suyo En efecto, sea

 $a \equiv b \pmod{m}$ ,  $a = a_1d$ ,  $b = b_1d = m \parallel m_1d$ 

Se tiene

$$a = b + mt$$
,  $a_1d = b_1d + m_1dt$ ,  $a_1 - b_1 + m_1t$ 

y, por lo tanto,  $a_1 = b_1 \pmod{m}$ .

c. Si se verifica la congruencia a me b respecto de varios módulos, entonces se verifica también respecto del módulo que es igual al minimo común múltiplo de estos módulos.

En efecto, de  $a = b \pmod{m_1}$ ,  $a = b \pmod{m_2}$ , ...  $a = b \pmod{m_b}$  se deduce que la diferencia a = b es divisible por todos los módulos  $m_1, m_2, \ldots, m_k$  Por esto, (c. § 3, cap. I), también es divisible esta diferencia por el mínimo común múltiplo m de estos módulos, es decir,  $a = b \pmod{m}$ . d. Si una congruencia se verifica respecto de un módulo m. también se verifica respecto de un módulo d que sea igual a cualauter divisor del número m.

En electo, de  $a = b \pmod{m}$  se deduce que la diferencia a = b tiene que ser divisible por m; por esto. (1, b, § 1, cap. I), esta diferencia tiene que ser divisible también por cualquier divisor d del número m, es decir, a = b (mód. d). e. Si un miembro de una congruencia y el módulo son divisibles por algún número, el otro miembro de la congruencia tiene que ser divisible por el mismo número.

En efecto, de  $a = b \pmod{m}$  se deduce que a - b + mt, si a y m son múltiplos de d, entonces (2, b, § 1, cap. I) también b tiene que ser múltiplo de d, como se afirmaba.

f. Si  $a = b \pmod{m}$ , entonces (a, m) = (b, m).

En efecto, en virtud de 2, b, § 2, cap. I, esta igualdad se deduce inmediatamente de a - b + mt

8 4. Sistema completo de restos

a. Los números que dan un mismo resto, o lo que es lo mismo, los que son congruentes respecto del módulo m, forman una

clase de números respecto del módulo m

De esta definición se deduce que a todos los números de una clase les corresponde un mismo resto r, por lo cual, haciendo recorrer a q en la forma mq + r todos los números enteros, se obtienen todos los números de la clase.

Correspondientemente a m valores distintos de r, se tienen m clases de números respecto del módulo m.

b. Cualquier número de la clase se llama resto o residuo respecto del módulo m con relación a todos los números de la misma clase. El resto que se obtiene para q=0, igual al residuo mismo r, se llama resto no negativo mínimo.

El resto p que es el menor en valor absoluto, se liama resto absoluto minimo.

Evidentemente, si  $r < \frac{m}{2}$  se tiene  $\rho = r$ ; si  $r > \frac{m}{2}$  se tiene  $\rho = r - m$ ; finalmente, si m es par y  $r = \frac{m}{2}$ , se puede tomar por  $\rho$  cualquiera de los dos números  $\frac{m}{2}$  y  $\frac{m}{2} - m = -\frac{m}{2}$ .

Tomando un resto de cada clase se obtiene un sistema completo de restos respecto del módulo m. Por lo general, como sistema completo de restos se emplean los restos no negativos mínimos  $0, 1, \ldots, m-1$  o también los restos absolutos mínimos; como se deduce de lo expuesto anteriormente, estos últimos, en caso de m impar, se representan por la sucesión

$$-\frac{m-1}{2}$$
, ...,  $-1$ ,  $0$ ,  $1$ , ...,  $\frac{m-1}{2}$ ,

y en el caso de m par, por una cualquiera de las dos sucesiones

$$-\frac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{m}{2}, \\ -\frac{m}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2}-1.$$

c. Cualesquiera m números que sean incongruentes dos a dos respecto del módulo m, forman un sistema completo de restos de este módulo.

En efecto, estos números, siendo incongruentes, tienen que pertenecer a distintas clases, y como en total hay m números,

es decir, tantos cuantas clases hay, en cada una de las clases tiene que haber, indudablemente, un número único.

d. Si (a, m) = 1 y x recorre el sistema completo de restos respecto del módulo m, entonces ax + b, donde b es un entero cualquiera, también recorre el sistema completo de restos respecto del módulo m.

En efecto, hay tantos números de la forma ax + b cuantos números x hay, es decir, m. Según c, no queda más que mostrar que dos números cualesquiera  $ax_1 + b$  y  $ax_2$  b, que corresponden a dos números incongruentes  $x_1$  y  $x_2$ , son también incongruentes entre sí respecto del módulo m.

Pero suponiendo que  $ax_1 + b \equiv ax_2 + b$  (mód m), se obtiene la congruencia  $ax_1 = ax_2$  (mód. m), de donde, en virtud de que (a, m) = 1, resulta  $x_1 = x_2$  (mód. m), lo cual contradice a la incongruencia de los números  $x_1 y x_2$ .

\$ 5. Sistema

reducido

de restos

a. En virtud de f, § 3, los números de

una misma clase respecto del módulo m

tienen con el módulo un mismo máximo

común divisor. Son de suma importancia las clases para

las cuales este divisor es igual a la unidad, es decir, las clases

que contienen números que son primos con el módulo.

Tomando sendos restos en estas clases, se obtiene el sistema reducido de restos respecto del módulo m. Por consiguiente, el sistema reducido de restos se puede formar de los números del sistema completo que son primos con el módulo. Ordinarlamente, el sistema reducido de restos se extrae del sistema de restos no negativos mínimos:  $0, 1, \ldots, m-1$ . Como entre estos hay  $\varphi(m)$  números que son primos con m, la cantidad de números del sistema reducido, así como la cantidad de clases que contienen números primos con el módulo, es igual a  $\varphi(m)$ 

Ejemplo. El sistema reducido de restos según el módulo 42 es

1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41

b. Cualesquiera  $\varphi$  (m) números que sean incongruentes dos a dos respecto del módulo m y que sean primos con el módulo, forman un sistema reducido de restos según el módulo m.

En efecto, estos números, siendo incongruentes dos a dos y primos con el módulo, tienen que pertenecer a distintas clases que contienen números que son primos con el módulo, y como en total hay  $\varphi$  (m) de tales números, es decir, tantos cuantas clases hay del tipo indicado, en cada una de las clases habrá, indispensablemente, un número único.

c. Si (a, m) = 1 y x recorre el sistema reducido de restos según el módulo m, ax también recorre el sistema reducido de restos según el módulo m.

En efecto, hay tantos números ax cuantos números x hay, es decir,  $\varphi$  (m). Por lo tanto, en virtud de b, no queda más que demostrar que los números ax son incongruentes dos a dos respecto del módulo m y son primos con el módulo Pero lo primero se demostró en d, § 4 para los números de la forma más general ax + b; lo segundo se deduce de que (a, m) = 1, (x, m) = 1.

§ 6. Teoremas a. Sim > 1 y (a, m) = 1 se tiene (teorema de Euler): y Fermat  $a \in Sim > 1$  y (a, m) = 1 se tiene (teorema de Euler):  $a \in Sim > 1$  y (a, m) = 1 se tiene (teorema de Euler):

En efecto, si x recorre el sistema reducido de restos

$$x = r_1, r_2, \ldots, r_c; c = \varphi(m),$$

formado por los restos no negativos mínimos, entonces los restos no negativos mínimos  $\rho_1, \rho_2, \dots, \rho_c$  de los números ax también recorren el mismo sistema, pero, generalmente, dispuestos en otro orden (c, § 5).

Multiplicando término a término las congruencias

$$ar_1 = \rho_1 \pmod{m}, ar_2 = \rho_2 \pmod{m}, \ldots,$$
  
 $ar_c = \rho_c \pmod{m},$ 

obtenemos

$$a^c r_1 r_2 \dots r_c = p_1 p_2 \dots p_c \pmod{m}$$
,

de donde, dividiendo ambos miembros por el producto  $r_1r_2\ldots r_n = \rho_1\rho_2\ldots \rho_n$ , resulta

$$a^c = 1 \pmod{m}$$
.

b. Si p es primo y a no es divisible por p, se tiene (teorema de Fermal):

$$a^{p-1} = 1 \pmod{p}, \tag{1}$$

Este teorema es una consecuencia del teorema a para m=p. Al último teorema se le puede dar una forma más cómoda. Precisando, si se multiplican ambos miembros de la congruencia (1) por a, se obtiene la congruencia

$$a^p = a \pmod{p}$$
.

sa cual es válida ya para todos los valores enteros de  $\alpha$ , puesto que también es válida si  $\alpha$  es múltiplo de  $\rho$ .

### Proguntas referentes al capitulo III

- a. Expresando los números enteros en el sistema decimal de numeración, deducir los criterios de divisibilidad por 3, 9, 11.
- b. Expresando los números enteros en el sistema de numeración de base 100, deducir el criterio de divisibilidad por 101.
- c. Expresando los números enteros en el sistema de numeración de base 1 000, deducir los criterios de divisibilidad por 37, 7, 11, 13.
- 2. Supongamos que m>0, (a, m)=1, b es entero, x recorre el Sistema completo y  $\xi$  el sistema reducido de restos respecto del módulo m: Demostrar que

a) 
$$\sum_{a} \left\{ \frac{ax+b}{m} \right\} = \frac{1}{2} (m-1),$$

$$\beta) \sum_{\mathbf{n}} \left\{ \frac{a\xi}{m} \right\} = \frac{1}{2} \, \varphi \left( m \right).$$

3, a. Supongamos que m > 0 (a, m) = 1,  $h \gg 0$ , c es real

$$S = \sum_{x=0}^{m-1} \left\{ \frac{ax + \psi(x)}{m} \right\},\,$$

donde  $\psi(x)$  para los valores considerados de x toma valores que cumplen la condición  $c \leqslant \psi(x) \leqslant c + h$ . Demostrar que

$$\left|S - \frac{1}{2}m\right| < h + \frac{1}{2}.$$

b. Supongamos que M es entero, m > 0, (a, m) = 1, A y B son reales,

$$A = \frac{a}{m} + \frac{\lambda}{m^3}; \quad S = \sum_{m=1}^{M+m-3} \{Ax + B\}.$$

Demostrar que

$$\left| S - \frac{1}{2} m \right| < |\lambda| + \frac{1}{2}.$$

c. Sea M entero, m > 0, (a, m) = 1,

$$S = \sum_{x=M}^{M+m-1} \{f(x)\},\,$$

donde la función f(x) admite derivadas continuas f'(x) y f'(x) en el intervalo  $M \le x \le M + m - 1$ , y se cumplen las condiciones

$$f'(M) = \frac{a}{m} + \frac{\theta}{m^2}$$
;  $(a, m) = 1$ ;  $|\theta| < 1$ ,  $\frac{1}{A} \le |f''(x)| \le \frac{k}{A}$ , siendo

$$1 \le m \le \tau$$
,  $\tau = A^{\frac{1}{5}}$ ,  $A > 2$ ,  $k > 1$ ,

Demostrar que

$$\left|S - \frac{1}{2}m\right| < \frac{k+3}{2}.$$

4. Supongamos que en el desarrollo del número irracional A en fracción continua todos los cocientes incompletos están acotados, M es entero, m es entero, m > 0, B es real.

Demostrar que

$$\sum_{n=M}^{M+m-1} (Ax+B) = \frac{1}{2} m + O(\ln m).$$

**5. a.** Supongamos que A > 2,  $k \ge 1$  y que la función f(x) admite derivada segunda continua en el intervalo  $Q \le x \le R$ , la cual satisface a las condiciones

$$\frac{1}{A} < |f'(x)| < \frac{k}{A}.$$

Demostrar que

$$\sum_{Q \leq x \leq R} (f(x)) = \frac{1}{2} (R - Q) + \theta \Delta; \quad |\theta| < 1.$$

$$\Delta = (2k^2(R-Q) \ln A + 8kA) A^{-\frac{1}{8}}.$$

b. Supongamos que  $0 < \sigma \le 1$ , Q y R son enteros. En las condiciones de la pregunta a, demostrar que el número  $\phi$  ( $\sigma$ ) de fracciones  $\{f(x)\}; x = Q + 1, \ldots, R$  con la condición  $0 \le f(x) < \sigma$  se expresa por la fórmula

$$\psi(\sigma) = \sigma(R - Q) + \theta' \cdot 2\Delta; \mid \theta' \mid < 1.$$

**6. a.** Sea T la cantidad de puntos enteros (x, y) que hay en la región  $x^3 + y^3 \le r^3$   $(r \ge 2)$ . Demostrar que

$$T = \pi r^2 + O(r^{\frac{1}{3}} \ln r).$$

**b.** Supongamos que n es entero, n > 2, E es la constante de Euler. Demostrar que

$$\tau(1) + \tau(2) + \ldots + \tau(n) = n(\ln n + 2E - 1) + O(n^{\frac{1}{2}}(\ln n)^2).$$

7. A un sistema de n números enteros positivos, en que cada número viene expresado en el sistema de numeración de base 2, lo llamaremos regular, si para cualquier entero no negativo s la cantidad de números, en cuya expresión figura 2º, es par, e irregular, si al menos para un s este número es impar

Demostrar que un sistema rregular se puede hacer regular disminuyendo o excluyendo completamente un solo término del mismo, y en sistema regular se hace irregular disminuyendo o excluyendo completamente cualquiera de sus térmi-

8, a. Demostrar que la forma

$$3^{n}x_{n} + 3^{n-1}x_{n-1} + \dots + 3x_{1} + x_{0}$$

donde  $x_n$ ,  $x_{n-1}$ , ...,  $x_1$ ,  $x_0$  recorren independientemente uno de otro los valores -1, 0, 1, representa todos los números

$$-H_1, \ldots, -1, 0, 1, \ldots, H_i, H = \frac{3^{n+1}-1}{3-1}$$

y, además, cada número, de un modo único.

b. Sean  $m_1, m_2, \ldots, m_h$  positivos, primos dos a dos. Aplicando c, § 4, demostrar que se obtiene el sistema completo de restos respecto del módulo  $m_1m_2, \ldots, m_h$ , haciendo recorrer a los números  $x_1, x_2, \ldots, x_h$  en la forma

$$x_1 + m_1x_2 + m_1m_2x_3 + \ldots + m_1m_2 \ldots m_{k-1}x_k$$

los sistemas completos de restos respecto de los módulos  $m_1, m_2, \ldots, m_h$ .

9. Sean  $m_1, m_2, \dots, m_k$  primes des a des y sea

$$m_1m_2$$
 .  $m_h = M_1m_1 = M_2m_2 = ... = M_km_k$ .

a. Aplicando c, § 4, demostrar que se obtiene el sistema completo de restos respecto del módulo  $m_1m_2 \ldots m_h$ , haciendo recorrer a los números  $x_1, x_2, \ldots, x_h$  en la forma

$$M_1x_1 + M_2x_2 + \ldots + M_kx_k$$

los sistemas completos de restos respecto de los módulos  $m_1, m_2, \ldots, m_k$ .

b. Aplicando c, § 4, cap. If y b, § 5, demostrar que se obtiene el sistema reducido de restos respecto del módulo  $m_1m_2$ ...  $m_{h_1}$  haciendo recorrer a los números  $x_1, x_2, \ldots, x_h$ 

en la forma

$$M_1x_1 + M_2x_2 + \ldots + M_kx_k$$

los sistemas reducidos de restos respecto de los módulos  $m_1, m_2, \ldots, m_k$ .

c. Demostrar el teorema de la pregunta b independientemente del teorema c, § 4, cap. Il y deducir entonces el último teorema como consecuencia del primero.

d. Hallar de un modo elemental la expresión para  $\varphi$  ( $p^{\alpha}$ ) y, aplicando la igualdad c, § 4, cap. II, deducir la expresión conocida para  $\varphi$  (a).

10. Sean  $m_1, m_2, \ldots, m_k$  primes dos a dos, superiores a 1,  $m = m_1 m_1 \ldots m_k$ ;  $m = M_n m_n$ .

a. Supongamos que  $x_1, x_2, \ldots, x_h, x$  recorren los sistemas completos de restos, y  $\xi_1, \xi_2, \ldots, \xi_h$ ,  $\xi$  los sistemas reducidos de restos respecto de los módulos  $m_1, m_2, \ldots, m_h, m$ . Demostrar que las fracciones

$$\left\{\frac{x_0}{m_1} + \frac{x_0}{m_0} + \dots + \frac{x_k}{m_k}\right\}$$

coinciden con las fracciones  $\left\{\frac{x}{m}\right\}$ , y las fracciones

$$\left\{ \frac{\xi_4}{m_1} + \frac{\xi_4}{m_1} + \ldots + \frac{\xi_k}{m_k} \right\}$$
 con las fracciones  $\left\{ \frac{\xi}{m} \right\}$ .

b. Sean dadas k funciones racionales enteras de coeficientes enteros de r variables  $x, \ldots, w(r > 1)$ :

$$f_{\theta}(x_1, \ldots, w) = \sum_{\alpha_1, \ldots, \alpha} c_{\alpha_s, \ldots, \alpha}^{(\theta)} x^{\alpha} \ldots w^{\delta}; \quad s = 1, \ldots, k,$$

y sea

$$f(x_1, \ldots, w) = \sum_{\alpha_1, \ldots, \delta} c_{\alpha_1, \ldots, \delta} x^{\alpha_1, \ldots, \delta};$$

$$c_{\alpha_1, \ldots, \delta} = \sum_{i=1}^{k} M_i c_{\alpha_i, \ldots, \delta}^{(i)};$$

 $x_{a_1}$  ...,  $w_{a_1}$  recorren los sistemas completos de restos y  $\xi_a$ , ...,  $\omega_a$  los sistemas reducidos de restos respecto del

módulo  $m_i$ ;  $x, \ldots, w$  recorren los sistemas completos de restos  $y \in \ldots, \omega$  los sistemas reducidos de restos respecto del módulo m. Demostrar que las fracciones

$$\left\{\frac{f_1\left(x_1,\ldots,w_l\right)}{m_1}+\ldots+\frac{f_k\left(x_k,\ldots,w_k\right)}{m_k}\right\}$$

coinciden con las fracciones  $\left\{\frac{f(x_1,...,w)}{m}\right\}$  y las fracciones

$$\left\{\frac{f_1\left(\xi_1,\ldots,\omega_1\right)}{m_1}+\ldots+\frac{f_k\left(\xi_k,\ldots,\omega_k\right)}{m_k}\right\}$$

con las fracciones  $\left\{\frac{f\left(\xi_{1},\ldots,\omega\right)}{m}\right\}$  (generalización de los teoremas de la pregunta a).

11, a. Supongamos que m es entero, m>0,  $\alpha$  es entero, x recorre el sistema completo de restos respecto del módulo m. Demostrar que

$$\sum e^{2\pi i \frac{ax}{m}} = \begin{cases} m, & \text{si } a \text{ es múltiplo de } m. \\ 0 \text{ en caso contrario.} \end{cases}$$

b.Supongamos que  $\alpha$  es real, M es entero, P es entero, P>0. Designando con la notación ( $\alpha$ ) el valor absoluto de la diferencia entre  $\alpha$  y el número entero más próximo a  $\alpha$  (distancia de  $\alpha$  al entero más próximo) demostrar que

$$\left|\sum_{x=aM}^{M+P-1} e^{2\pi i \alpha x}\right| \leqslant \min\left(P, \frac{1}{h\left(\alpha\right)}\right); \quad h \geqslant \begin{cases} 2 \text{ siempre} \\ 3, \text{ si } (\alpha) \leqslant \frac{1}{6}. \end{cases}$$

c. Supongamos que m es entero, m > 1 y que las funciones M(a) y P(a) para los valores a = 1, 2, ..., m - 1 toman valores enteros con la condición P(a) > 0. Demostrar que

$$\sum_{\alpha=1}^{m-1} \left| \sum_{x=M(\alpha)}^{M(\alpha)+P(\alpha)-1} e^{2\pi i \frac{x}{m}x} \right| < \begin{cases} m \ln m - \frac{m}{3} \ln \left( 2 \left[ \frac{m}{6} \right] + 1 \right), \\ m \ln m - \frac{m}{2}, & \text{si } m > 12, \\ m \ln m - m, & \text{si } m > 60. \end{cases}$$

12, a. Supongamos que m es entero, m>0,  $\xi$  recorre el sistema reducido de restos respecto del módulo m. Demostrar que

$$\mu(m) = \sum_{k} e^{2\pi i \frac{k}{m}}.$$

- b. Aplicando el teorema de la pregunta a, demostrar el primero de los teoremas c, § 3, cap. II (véase la resolución de la pregunta 28, a, cap. II).
- c. Deducir el teorema de la pregunta a, aplicando el teorema de la pregunta 17, a, cap. II.
- d. Supongamos que

$$f(x,\ldots,w) = \sum_{\alpha,\ldots,\delta} c_{\alpha},\ldots,x^{\alpha}\ldots w^{\delta}$$

es una función racional entera de coeficientes enteros de r variables  $x, \ldots, w$   $(r \ge 1), a$  es entero, m es entero, m > 0;  $x, \ldots, w$  recorren el sistema completo de restos  $y \ \xi, \ldots, \omega$  el sistema reducido de restos respecto del módulo m. Introducimos las notaciones

$$S_{a, m} := \sum_{n} \dots \sum_{i=1}^{n} e^{\frac{2\pi i}{n} \frac{af(x, \dots, w)}{m}},$$
  
$$S'_{a, m} := \sum_{i=1}^{n} \dots \sum_{i=1}^{n} e^{\frac{2\pi i}{n} \frac{af(x, \dots, w)}{m}}.$$

Supongamos también que  $m=m_1 \ldots m_k$ , donde  $m_1, \ldots, m_k$  son primos dos a dos, superiores a 1, y sea  $m=M_0m_0$ . Demostrar que

$$S_{a_1, m_1} \dots S_{a_h, m_h} = S_{M_1 a_1 + \dots + M_h a_h, m},$$
  
 $S'_{a_1, m_1} \dots S'_{a_h, m_h} = S'_{M_1 a_1 + \dots + M_h a_h, m}.$ 

e. Con las notaciones de la pregunta d, hacemos

$$A(m) = m^{-r} \sum_{a} S_{a, m}, \quad A'(m) = m^{-r} \sum_{a} S'_{a, m},$$

donde a recorre el sistema reducido de restos respecto del módulo m Demostrar que

$$A(m_1) \dots A(m_h) = A(m),$$
  
 $A'(m_1) \dots A'(m_h) = A'(m).$ 

13, a. Demostrar que

$$\varphi\left(a\right) = \sum_{n=0}^{a-1} \prod_{n} \left(1 - \frac{1}{\rho} \sum_{n=0}^{p-1} e^{2\pi i \frac{n \cdot k}{p}}\right),$$

donde p recorre los divisores primos del número a.

b. Deducir la expresión conocida para  $\phi$  (a) de la identidad de la pregunta a.

14. Demostrar que

$$\tau(a) = 2 \sum_{0 < \pi < V_a} \frac{1}{x} \sum_{h=0}^{\pi - 1} e^{2\pi i \frac{ah}{x}} + \delta_i$$

donde  $\delta = 1$   $\delta$   $\delta = 0$ , según que a sea el cuadrado de un número entero o no lo sea.

15, a. Supongamos que p es primo y  $h_1, h_2, \ldots, h_n$  son enteros. Demostrar que

$$(h_1 + h_2 + \dots + h_n)^p =$$
  
=  $h_1^p + h_2^p + \dots + h_n^p \pmod{p}$ .

b. Deducir el teorema de Fermat del teorema de la pregunta a.

c. Deducir el teorema de Euler del teorema de Fermat.

### Ejercicios numéricos referentes ai capitulo III

1, a. Hallar el resto de la división de

b. ¿Es divisible el número 2º es -2 por 1 093º?

2, a. Aplicando los criterios de divisibilidad dela pregunta 1, haliar

el desarrollo canónico del número 244 943 325

b. Hallar el desarrollo canónico del número 282 321 246 671 737,

### CAPITULO CUARTO

## Congruencias con una incógnita

§ 1. Conceptos Nuestro objetivo próximo es el estudio fandamentales de las congruencias de la siguiente forma general:

 $f(x) = 0 \pmod{m}$ ;  $f(x) = ax^n + a_1x^{n-1} + \ldots + a_n(1)$ Si a no es divisble por m, el número n se llama grado de la congruencia.

Resolver la congruencia, significa hallar todos los valores de x que la satisfacen. Dos congruencias, a las que satisfacen unos mismos valores de x, se llaman equivalentes.

Si a la congruencia (1) la satisface algún  $x=x_1$ , entonces (d. § 2, cap. III) a la misma congruencia la satisfacen también todos los números que son congruentes con  $x_1$  respecto del módulo  $m: x = x_1$  (mód. m). Toda esta clase de números se considera como una solución. Por lo tanto, la congruencia (1) tendrá tantas soluciones cuantos restos del sistema completo la satisfagan.

Ejemplo. A la congruencia

$$x^6 + x + 1 = 0 \text{ (mod. 7)},$$

entre los números 0, 1, 2, 3, 4, 5, 6 del sistema completo de restos respecto del módulo 7, la satisfacen dos números: x = 2 y x = 4. Por ello, la congruencia indicada tiene dos soluciones:

 $x = 2 \text{ (mod. 7)}, \quad x = 4 \text{ (mod. 7)}.$ 

§ 2. Congruencias

de primer grado

de primer grado

diente (con el signo contrario) al segundo

miembro, se reduce a la forma

$$ax = b \pmod{m}$$
, (1)

- b. Comenzando a estudiar el problema del número de soluciones de la congruencia (1), nos limitaremos primero al caso (a, m) = 1. En virtud del § 1, la congruencia considerada admite tantas soluciones cuantos restos del sistema completo la satisfacen Mas, cuando x recorre el sistema completo de restos respecto del módulo m, ax recorre el sistema completo de restos (d, § 4, cap. III). Por consiguiente, para un valor de x tomado del sistema completo, y sólo para uno, ax será congruente con b. Así, pues, si (a, m) = 1 la congruencia (1) admite una sola solución.
- c. Supongamos ahora que (a, m) d > 1. Entonces, para que la congruencia (1) tenga solución es necesario (c, § 3, cap. III) que b sea divisible por d, pues en caso contrario la congruencia (1) sería imposible para algún x entero. Por esta razón, suponiendo que b es un múltiplo de d, hacemos  $a = a_1d$ ,  $b = b_1d$ ,  $m = m_1d$ . Entonces la congruencia (1) (después de haber simplificado por d) resulta equivalente a  $a_1x = b_1$  (mód.  $m_1$ ), en la cual  $(a_1, m_1) = 1$  y, por lo tanto admite una solución respecto del módulo  $m_1$ . Sea  $m_1$  el resto no negativo mínimo de esta solución respecto del módulo  $m_2$ , entonces todos los números  $m_2$  que forman esta solución serán de la forma

$$x = x_1 \pmod{m_1}. \tag{2}$$

Respecto del módulo m los números (2) forman más de una solución, forman precisamente tantas soluciones cuantos números (2) haya en la sucesión  $0, 1, 2, \dots, m-1$  que sean restos no negativos mínimos respecto del módulo m. Tales números son:

$$x_1, x_1 + m_1, x_1 + 2m_1, \dots, x_n + (d-1) m_1$$

es decir, en total d numeros (2) v. por consiguiente, la congruencia (1) admite d soluciones.

d. Haciendo un resumen de todo lo demostrado, resulta el teorema signiente:

Sea (a, m) = d. La congruencia  $ax = b \pmod{m}$  es imposible si b no es divisible por d. Si b es múltiplo de d, la congruencia admite d soluciones.

e. Para averiguar las soluciones de la congruencia (1), indicaremos solamente un método, basado en la teoría de las fracciones continuas; además, es suficiente limitarse al caso (a, m) = 1.

Desarrollando en fracción continua la razón m: a,

en fracción continua la razón 
$$m$$

$$\frac{m}{a} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \dots + \frac{1}{q_n}}} \cdot \cdot + \frac{1}{q_n}$$

y considerando las dos fracciones reducidas últimas:

$$\frac{P_{n-1}}{Q_{n-1}}, \quad \frac{P_n}{Q_n} = \frac{m}{a},$$

en virtud de las propiedades de las fracciones continuas (e, § 4, cap. 1), se tiene:

$$mQ_{n-1} - aP_{n-1} = (-1)^n,$$
  
 $aP_{n-1} = (-1)^{n-1} \text{ (mod. m)},$   
 $a \cdot (-1)^{n-1}P_{n-1}b = b \text{ (mod. m)}.$ 

Así, pues, la congruencia en cuestión admite la solución  $x = (-1)^{n-1}P_{n-1}b \pmod{m}$ .

para cuya averiguación es suficiente calcular  $P_{n-1}$  según el método señalado en d. 6 4, cap. 1.

Ejempto. Resolvamos la congruencia

$$111x = 75 \text{ (mod. 321)}. \tag{3}$$

Agui (111,321) = 3, siendo 75 múltiplo de 3. Por esta razón, la congruencia admite tres soluciones.

Dividiendo ambos miembros de la congruencia y el módulo por 3, obtenemos la congruencia

$$37x = 25 \pmod{107}$$
, (4)

la cual debe resolverse primeramente. Se tiene

q		2	1	8	4
Pa	1	2	3	26	107

Por lo tanto, en el caso dado n=4,  $P_{n-1}=26$ , b=25, y obtenemos la solución de la congruencia (4) en la forma  $x=-26\cdot25=99$  (mód. 107).

De aquí, las soluciones de la congruencia (3) se expresan así: x = 99: 99 + 107: 99 + 2·107 (mód. 321).

es decir.

x = 99; 206; 313 (mód. 321).

§ 3. Sistema a. Estudiaremos solamente el sistema más simple de congruencias  $x = b_1 \pmod{m}$ .

$$x = b_1 \pmod{m_1}, \ldots, x = b_k \pmod{m_k}$$
 (1)

con una incógnita, pero con distintos módulos que son primos dos a dos.

b. Se puede resolver el sistema (1), es decir, se pueden hallar todos los valores de x que le satisfacen, aplicando el teorema siguiente: Supongamos que los números M, y M', vienen definidos por las condiciones

$$m_1m_2$$
 . .  $m_k = M_sm_s$ ,  $M_sM_s' = 1 \pmod{m_s}$ 

*y 88*a

$$x_0 = M_1 M_1 b_1 + M_2 M_2 b_2 + \ldots + M_k M_k b_k$$

Entonces el conjunto de valores de x que satisfacen al sistema (1) se determina por la congruencia

$$x = x_0 \pmod{m_1 m_2} \qquad m_k \qquad (2)$$

En efecto, como todos los números  $M_i$ , distintos de  $M_s$ , son divisibles por  $m_s$ , para cualquier  $s=1,\,2,\,\ldots,\,k$  se tiene

$$x_0 = M_a M_a' b_a \equiv b_a \pmod{m_a}$$

y, por consignmente, el sistema (i) es equivalente al sistema  $x = x_0 \pmod{m_1}, x = x_0 \pmod{m_2}, \dots$ 

$$\dots x = x_n \pmod{m_k} \quad (3)$$

(es decir, a los sistemas (1) y (3) les satisfacen unos mismos valores de x). Pero, en virtud de los teoremas c, § 3, cap. III y d, § 3, cap. III, al sistema (3) le satisfacen aquellos valores de x, y sólo aquellos, que satisfacen a la congruencia (2). c. Si  $b_1$ ,  $b_2$ , ...,  $b_k$  recorren independientemente uno de otro los sistemas completos de restos respecto de los módulos  $m_1$ ,  $m_2$ , ...,  $m_k$ , entonces  $x_0$  recorre el sistema completo de restos respecto del módulo  $m_1 m_2 \ldots m_k$ .

En efecto,  $x_0$  recorre  $m_1m_2 \ldots m_k$  valores, los cuales, en virtud de d, § 3, cap. III, son incongruentes respecto del módulo  $m_1m_2 \ldots m_k$ .

d. Ejemplo. Resolvamos el sistema

$$x = b_1 \pmod{4}, \quad x = b_2 \pmod{5}, \quad x = b_3 \pmod{7}.$$

Aquí 4.5.7 = 35.4 = 28.5 = 20.7, y además,

$$35.3 = 1 \pmod{4}$$
,  $28.2 = 1 \pmod{5}$ ,

$$20.6 \equiv 1 \pmod{7}$$

Por lo tanto

$$x_0 = 35 \cdot 3b_1 + 28 \cdot 2b_2 + 20 \cdot 6b_3 - 105b_1 + 56b_2 + 120b_3$$

y, por consiguiente, el conjunto de valores de x que satisfacen al sistema puede expresarse en la forma

$$x = 105b_1 + 56b_2 + 120b_2 \pmod{140}$$

Por elemplo, el conjunto de valores de x que satisfacen al sistema

$$x = 1 \pmod{4}$$
,  $x = 3 \pmod{5}$ ,  $x = 2 \pmod{7}$ .

es

$$x = 105 \cdot 1 + 56 \cdot 3 + 120 \cdot 2 = 93 \pmod{140}$$

y el conjunto de valores de x que satisfacen al sistema  $x \equiv 3 \pmod{4}, \quad x \equiv 2 \pmod{5}, \quad x \equiv 6 \pmod{7},$ 

68

primo

$$x = 105.3 + 56.2 + 120.6 \approx 27 \pmod{140}$$

a. Sea p un número primo. Demostremos § 4. Congruenclas de cualquier grado respecto de un módulo

unos teoremas generales relativos a una congruencia de la forma

$$f(x) = 0 \text{ (mod. } p),$$

$$f(x) = ax^n + a_1x^{n-1} + \dots + a_n$$
 (1)

b. Una congruencia de la forma (1) es equivalente a una congruencia de grado no superior a p - 1.

En efecto, dividiendo f(x) por  $x^p - x$ , se tiene

$$f(x) = (x^p - x) Q(x) + R(x).$$

donde el grado de R(x) no es superior a p-1 Como  $x^p-x=$  $0 \pmod{p}$ , resulta  $f(x) = R(x) \pmod{p}$ , de donde se

deduce el teorema indicado. c. Si la congruencia (1) admite más de n soluciones, todos los

coeficientes de f (x) son múltiplos de p.

En efecto, supongamos, que la congruencia (1) admite al menos n + 1 soluciones. Designando los restos de estas soluciones con las letras  $x_1$ ,  $x_2$ , . . ,  $x_n$ ,  $x_{n+1}$ , podemos expresar f(x) en la forma

$$f(x) = a(x - x_1)(x - x_2) \dots (x - x_{n-2})(x - x_{n-1})(x - x_n) + + b(x - x_1)(x - x_2) \dots (x - x_{n-2})(x - x_{n-1}) + + c(x - x_1)(x - x_2) \dots (x - x_{n-2}) + + \dots \dots \dots \dots + + k(x - x_1)(x - x_3) + + l(x - x_1) + + m,$$
 (2)

Con este fin, transformando (abriendo paréntesis) los sumandos del segundo miembro en polinomios, elegimos b de tal modo que la suma de los coeficientes de  $x^{n-1}$  en los dos primeros polinomios coincida con  $a_1$ ; una vez hallado b, elegimos c de tal modo que la suma de los coeficientes de  $x^{n-1}$  en los primeros tres polinomios coincida con  $a_2$ , etc

Haciendo en (2)  $x = x_1, x_2, \ldots, x_n, x_{n+1}$ , sucesivamente, comprobamos que todos los números  $m, l, k, \ldots, c, b, a$  son múltiplos de p. Por lo tanto, también son múltiplos de p todos los números  $a, a_1, \ldots, a_n$  (como sumas de números que son múltiplos de p).

 d. Si p es un número primo, se verifica la congruencia (teorema de Wilson)

$$1 \cdot 2 \dots (p-1) + 1 \equiv 0 \pmod{p}$$
 (3)

En efecto, si p = 2 el teorema es evidente. Si p > 2 consideramos la congruencia

$$(x-1)(x-2)$$
 .  $(x-(p-1))-(x^{p-1}-1)=$  = 0 (mód. p),

ésta es de grado no superior a p-2 y admite p-1 soluciones; precisamente las soluciones cuyos restos son 1, 2, ..., p-1. Por consiguiente, según el teorema o todos sus coeficientes son múltiplos de p, en particular, también es

divisible por p el término independiente, el cual es precisamente igual al primer miembro de la congruencia (3). **Ejemplo.** Se tiene  $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 + 1 = 721 \equiv 0 \pmod{7}$ .

§ 5. Congruenctas
de cualquier
grado respecto
de un módulo
compuesto

a. Si  $m_1, m_2, \ldots, m_k$  son primos dos a
dos, la congruencia  $f(x) \equiv 0 \pmod{m_1 m_2 \ldots m_k}$ es equivalente al sistema  $f(x) \equiv 0 \pmod{m_1}.$ 

$$f(x) \equiv 0 \pmod{m_2}, \ldots, f(x) \equiv 0 \pmod{m_k}.$$

Además, designando con  $T_1, T_2, \ldots, T_k$  los números de soluciones de cada una de las congruencias de este sistema respecto de los módulos correspondientes y con T el número de soluciones de la congruencia (1), se tiene

$$T = T_1 T_2 \dots T_k$$

Eπ efecto, la primera parte del teorema se deduce de c y d, § 3, cap. III. La segunda parte se deduce de que cada una de las congruencias

$$f(x) \equiv 0 \text{ (mod. } m_a) \tag{2}$$

se cumple cuando, y sólo cuando, se cumple una de las  $T_{\rm a}$  congruencias de la forma

$$x \equiv b_s \pmod{m_s}$$

donde  $b_a$  recorre los restos de las soluciones de la congruencia (2); además, son posibles en total  $T_1T_2$  .  $T_k$  combinaciones distintas de la forma

 $x = b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \quad x = b_k \pmod{m_k},$  que dan lugar (c, § 3) a clases distintas respecto del módulo

$$m_1m_2$$
 . . .  $m_k$ 

Ejempio. La congruencia

$$f(x) \equiv 0 \pmod{35}, \quad f(x) = x^4 + 2x^3 + 8x + 9$$
 (3)

es equivalente al sistema

$$f(x) \equiv 0 \pmod{5}$$
,  $f(x) \equiv 0 \pmod{7}$ .

Fácilmente se comprueba (§ 1) que la primera congruencia de este sistema tiene 2 soluciones: x = 1; 4 (mód 5), la segunda congruencia tiene 3 soluciones: x = 3; 5, 6 (mód. 7). Debido a esto, la congruencia (3) tiene  $2 \cdot 3 = 6$  soluciones. Para hallar estas 6 soluciones, hay que resolver 6 sistemas de la forma

$$x \equiv b_1 \pmod{5}, \quad x \equiv b_2 \pmod{7},$$
 (4)

las cuales se obtienen haciendo recorrer a  $b_1$  los valores  $b_1 = 1, 4, y$  a  $b_2$  los valores  $b_2 = 3; 5; 6$  Pero, como

 $35 = 7 \cdot 5 = 5 \cdot 7$ ,  $7 \cdot 3 \equiv 1 \pmod{5}$ ,  $6 \cdot 3 \equiv 1 \pmod{7}$ , el conjunto de valores de x que satisfacen al sistema (4) se expresa en la forma (5, § 3)

$$x = 21b_1 + 15b_2 \pmod{.35}$$

Por lo tanto, las soluciones de la congruencia (3) son x == 31; 26; 6; 24; 19; 34 (mód. 35).

 b. En virtud del teorema a, la discusión y solución de la congruencia

$$f(x) = 0 \pmod{p_1^{\alpha_1}p_2^{\alpha_2} \dots p_k^{\alpha_k}}$$

se reduce a la discusión y solución de las congruencias de la forma

$$f(x) = 0 \text{ (mod. } p^a); \tag{5}$$

como ahora aclararemos, esta última congruencia se reduce en general a la congruencia

$$f(x) = 0 \text{ (mod. } p). \tag{6}$$

En efecto, todo x que satisface a la congruencia (5) necesariamente tiene que satisfacer también a la congruencia (6) Sea

$$x = x_1 \pmod{p}$$

alguna solución de la congruencia (6). Entonces  $x = x_i +$ + pt, donde t, es entero. Poniendo este valor de x en la congruencia

 $f(x) = 0 \pmod{p^3}$ 

y desarrollando el primer miembro según la fórmula de Taylor, hallamos (teniendo en cuenta que  $\frac{1}{k!} f^{(k)}(x_k)$  es entero y despreciando los términos que son múltiplos de p3):  $f(x_1) + pt_1f'(x_1) = 0 \pmod{p^2}, \frac{f(x_1)}{p} + t_1f'(x_1) = 0 \pmod{p}.$ Limitándonos aquí al caso en que  $f'(x_i)$  no es divisible por p, resulta una solución:

$$t_1 = t'_1 \pmod{p}$$
;  $t_1 = t'_1 + \rho t_2$ .

La expresion de x toma la forma

$$x = x_1 + pt_1' + p^2t_2 - x_2 + p^2t_2;$$

ponténdola en la congruencia

$$f(x) \equiv 0 \pmod{p^3},$$

resulta

$$\begin{split} f(x_3) + \rho^2 \ell_3 f'(x_2) &= 0 \text{ (mód. } \rho^3), \\ \frac{f(x_3)}{\rho^2} + \ell_3 f'(x_3) &= 0 \text{ (mód. } \rho). \end{split}$$

Agul  $f'(x_2)$  no es divisible por p, puesto que  $x_1 = x_1 \pmod{p}$ .

$$f'(x_2) \approx f'(x_1) \pmod{p}$$
,

y, por lo tanto, la última congruencia tiene una sola solución:

$$t_1 = t'_1 \pmod{p};$$
  
$$t_2 = t'_1 + pt_2.$$

La expresión de x toma la forma

$$x = x_2 + p^3t_3' + p^3t_3 = x_3 + p^3t_3;$$

etc. De este modo, partiendo de la solución dada de la congruencia (6) haliamos la solución congruente con ella de la

congruencia (5). En resumen, toda solución  $x = x_1 \pmod{p}$  de la congruencia (6), con la condición de que  $f'(x_1)$  no sea divisible por p, proporciona una solución de la congruencia (5):

$$x = x_{\alpha} + p^{\alpha} l_{\alpha};$$
  
 $x \equiv x_{\alpha} \pmod{p^{\alpha}}.$ 

Ejemplo. Resolvamos la congruencia

$$\begin{cases}
f(x) \equiv 0 \text{ (mod. 27);} \\
f(x) = x^4 + 7x + 4.
\end{cases}$$
(7)

La congruencia f(x) = 0 (mód. 3) tiene una solución x = 1 (mód. 3); en este caso f'(1) = 2 (mód. 3) y, por consiguente, no es divisible por 3. Hallamos:

$$x = 1 + 3t_1,$$

$$f(1) + 3t_1 f'(1) = 0 \pmod{9}, \ 3 + 3t_1 \cdot 2 = 0 \pmod{9},$$

$$2t_1 + 1 = 0 \pmod{3}, \ t_1 = 1 \pmod{3}, \ t_2 = 1 + 3t_2,$$

$$x = 4 + 9t_2,$$

$$f(4) + 9t_3f'(4) = 0 \pmod{27}, 18 + 9t_3 \cdot 2 = 0 \pmod{27},$$
  
 $2t_2 + 2 = 0 \pmod{3}, t_3 = 2 \pmod{3}, t_2 = 2 + 3t_3,$   
 $x = 22 + 27t_3.$ 

Por lo tanto, la congruencia (7) tiene una solución x == 22 (mód. 27).

## Preguntas referentes al capitulo IV

**1, a.** Supongamos que m es entero, m>0,  $f(x, \ldots, w)$  es una función racional entera de r variables  $x, \ldots, w$   $(r\geqslant 1)$  con coeficientes enteros. Si el sistema  $x=x_0, \ldots, w=w_0$  satisface a la congruencia

$$f(x, \ldots, w) = 0 \text{ (mod. } m) \tag{1}$$

entonces (generalización de la definición del § 1), el sistema de clase de números respecto del módulo m:

$$x = x_0 \pmod{m}, \ldots, w = w_0 \pmod{m}$$

lo consideramos como una solución de la congruencia (1). Sea T el número de soluciones de la congruencia (1). Demostrar que

$$Tm = \sum_{n=0}^{m-1} \sum_{n=0}^{m-1} \dots \sum_{n=0}^{m-1} e^{innt} \frac{a_f(x, \dots, \omega)}{m},$$

 b. Con las notaciones de la pregunta a y de la pregunta 12, e, cap. III, demostrar que

$$Tm = m^{\tau} \sum_{m_0 \searrow m} A(m_0).$$

 c. Aplicar la igualdad de la pregunta a para demostrar el teorema del número de soluciones de una congruencia de primer grado.

d. Supongamos que m es entero, m > 0;  $a, \ldots, f, g$  son enteros, en total r + 1 súmeros (r > 0);  $d = (a, \ldots, f, m)$ ; T es el número de soluciones de la congruencia

$$ax + \ldots + fw + g = 0 \pmod{m}$$
.

Aplicando la igualdad de la pregunta, a, demostrar que

$$T = \left\{ \begin{array}{ccc} m^{r-1} d, & \text{si } g \text{ es } \text{múltiplo } \text{de } d, \\ 0 & \text{en } \text{caso } \text{contrario}. \end{array} \right.$$

- e. Demostrar el teorema de la pregunta d partiendo del teorema del número de soluciones de la congruencia ax = = b (môd. m).
- 2, a. Sea m > 1, (a, m) = 1. Demostrar que la congruencia  $ax = b \pmod{m}$  admite la solución  $x = ba^{-(m)-1} \pmod{m}$ . b. Sea p un número primo, 0 < a < p. Demostrar que la congruencia  $ax = b \pmod{p}$  admite la solución

$$x = b (-1)^{a-1} \frac{(p-1)(p-2) \dots (p-a+1)}{1 \cdot 2 \dots a}$$
 (mód. p).

 c. α) Indicar el método más simple posible de resolución de una congruencia de la forma

$$2^h x = b \pmod{m}$$
;  $(2, m) = 1$ .

β) Indicar el método más simple posible de resolución de la congruencia

 $3^{h}x \equiv b \pmod{m}$ ; (3, m) = 1.

- $\gamma$ ) Sea (a, m) = 1, 1 < a < m. Desarrollando los métodos indicados en las preguntas  $\alpha$ ) y  $\beta$ ), demostrar que la búsqueda de la solución de la congruencia  $ax = b \pmod{m}$  puede reducirse a la búsqueda de las soluciones de congruencias de la forma  $b + mt = 0 \pmod{p}$ , donde p es un divisor primo del número a.
- 3. Sea m entero, m > 1,  $1 \le \tau < m$ , (a, m) = 1. Empleando la teoria de congruencias, demostrar la existencia de enteros  $x \in y$  con las condiciones

$$ax = y \pmod{m}, \quad 0 < x \leqslant \tau, \quad 0 < |y| < \frac{m}{\tau}.$$

- **4. a.** Siendo (a, m) = 1, consideramos la fracción simbólica  $\frac{b}{a}$  respecto del módulo m, la cual denota cualquier resto de la solución de la congruencia  $ax = b \pmod{m}$ . Demostrar (las congruencias se toman respecto del módulo m) que:
- a) Si  $a = a_i$ ,  $b = b_i$ , se tiene  $\frac{b}{a} = \frac{b_i}{a_i}$ .
- β) El numerador b de la fracción simbólica  $\frac{b}{a}$  se puede sustituir por un número congruente  $b_0$ , múltiplo de a. Entonces, la fracción simbólica  $\frac{b}{a}$  es congruente con el número entero que se expresa por la fracción ordinaria  $\frac{b_0}{a}$ .
- $\gamma \rangle = \frac{b}{a} + \frac{d}{c} = \frac{bc + ad}{ac}.$
- $\delta) \ \frac{b}{a} \cdot \frac{d}{a} = \frac{bd}{ac}.$
- b,  $\alpha$ ) Supongamos que p es primo, p > 2, a es entero, 0 < a < p-1. Demostrar que

$$\binom{p-1}{a} = (-1)^a \pmod{p}.$$

- β) Sea p un número primo, p > 2. Demostrar que  $\frac{2p-2}{p} = 1 \frac{1}{2} + \frac{1}{3} \dots \frac{1}{p-1} \text{ (mód. } p\text{)}.$
- 5, a. Sea d un divisor del número a, que no sea divisible por el cuadrado de un número entero superior a 1 y tampoco por los números primos menores que n, y sea x el número de divisores primos distintos del número d. Demostrar que en la sucesión

$$1 \cdot 2 \cdot \ldots \cdot n$$
,  $2 \cdot 3 \cdot \ldots \cdot (n+1)$ ,  $\ldots$ ,  $a(a+1) \cdot \ldots \cdot (a+n-1)$  (1) hay  $\frac{n^n a}{d}$  números que son múltiplos de  $d$ .

b. Sean  $p_1, p_2, \ldots, p_k$  los divisores primos distintos del número a, donde ninguno de ellos es inferior a n. Demostrar

número a, donde ninguno de ettos es inferior a n. Demostrar que la cantidad de números de la sucesión (1) que son primos con a, es igual a

$$a\left(1-\frac{n}{p_1}\right)\left(1-\frac{n}{p_2}\right)\ldots\left(1-\frac{n}{p_k}\right)$$

6. Sea  $m_{1, 3}, \ldots, k$  el mínimo común múltiplo de los números  $m_1, m_2, \ldots, m_k$ .

a. Supongamos que  $d = (m_i, m_i)$ . Demostrar que el sistema

$$x = b_1 \pmod{m_1}, \quad x = b_2 \pmod{m_0}$$

admite solución, y sólo cuando,  $b_3 - b_1$  es múltiplo de d. Además, cuando admite solución, el conjunto de valores de x que satisfacen a este sistema se determina por una congruencia de la forma

$$x = x_{1,2} \pmod{m_{1,2}}$$
.

b. Demostrar que en caso de que el sistema  $x \equiv b_1 \pmod{m_1}, x \equiv b_2 \pmod{m_2}, \ldots, x \equiv b_k \pmod{m_k}$  admita solución, el conjunto de valores x que le satisfacen se determina por una congruencia de la forma

$$x = x_1, x_2, \dots, x_n \pmod{m_{1, 1}, \dots, x_n}.$$

7. Supongamos que m es entero, m > 1, a y b son enteros,

$$\left(\frac{a, b}{m}\right) = \sum_{x} e^{2\pi i \frac{ax + bx^{x}}{m}}$$

donde x recorre el sistema reducido de restos respecto del módulo m, y  $x' = \frac{1}{x} \pmod{m}$  (en el sentido de la pregunta 4, a). Demostrar las siguientes propiedades del símbolo  $\left(\frac{a,b}{m}\right)$ :

ca) 
$$\left(\frac{a, b}{m}\right)$$
 es real.

$$\beta) \left( \frac{a, b}{m} \right) = \left( \frac{b, a}{m} \right).$$

$$\gamma$$
) Si  $(h, m) = 1$  se tiene  $\left(\frac{a, bh}{m}\right) := \left(\frac{ah, b}{m}\right)$ .

6) Si  $m_1, m_2, \ldots, m_k$  son primes des a des, haciendo  $m_1, m_2 \ldots m_k = m, M - M_{\theta} m_{\theta}$ , se tiene

$$\left( \frac{a_{1}, 1}{m_{1}} \right) \left( \frac{a_{1}, 1}{m_{2}} \right) \dots \left( \frac{a_{k}, 1}{m_{k}} \right) = \\ = \left( \frac{M_{1}^{2} a_{1} + M_{1}^{2} a_{2} + \dots + M_{k}^{2} a_{k}, 1}{m} \right) .$$

8. Supongamos que la congruencia

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0 \pmod{\rho}$$

admite a soluciones

$$x = x_1, x_2, \ldots, x_n \pmod{\rho}$$
.

Demostrar que

$$a_1 = -a_0 S_1 \pmod{p},$$

$$a_2 = a_0 S_2 \pmod{p},$$

$$a_3 = -a_0 S_3 \pmod{p},$$

$$a_1 = -a_0 S_3 \pmod{p},$$

$$a_n = (-1)^n a_0 S_n \pmod{p},$$

donde  $S_1$  es la suma de todas las  $x_s$ ,  $S_2$  es la suma de sus productos dos a dos,  $S_3$  es la suma de sus productos tres a tres, etc.

- 9, a. Demostrar el teorema de Wilson, considerando los pares de números x, x' de la sucesión 2, 3, . . ., p-2, que satisfacen a la condición xx' = 1 (mód. p).
- b. Sea P entero,  $P > 1, 1, 2 \dots (P 1) + 1 = 0 \pmod{P}$ . Demostrar que P es primo.
- 10, a. Sea  $(a_0, m) = 1$ . Indicar una congruencia de n-ésimo grado con el coeficiente superior igual a 1, que sea equivalente a la congruencia

$$a_0x^n + a_1x^{n-1} + \dots + a_n = 0 \pmod{m}$$
.

- b. Demostrar que la condición necesaria y suficiente para que la congruencia  $f(x) = 0 \pmod{p}$ ;  $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ ;  $n \leq p$ , admita n soluciones, es que sean divisibles por p todos los coeficientes del resto de la división de  $x^p x$  por f(x).
- c. Set n un divisor de p-1, n>1, (A, p)=1. Demostrar que la condición necesaria y suficiente para que sea resoluble la congruencia  $x^n \equiv A \pmod{p}$  es que se cumpla la con-
- gruencia  $A^{\frac{p-1}{n}} = 1$  (mód.  $\rho$ ); además, en caso de resolubilidad, la congruencia indicada admite n soluciones.
- 11. Supongamos que n es entero, n > 0, (A, m) = 1, y que se conoce una solución  $x = x_0$  (mód. m) de la congruencia  $x^n = A$  (mód. m). Demostrar que todas las soluciones de esta congruencia se expresan por el producto de  $x_0$  por los restos de las soluciones de la congruencia  $y^n = 1$  (mód. m).

## Ejercicios numéricos referentes al capitalo IV

- 1, a. Resolver la congruencia 256x 179 (mód 337)
- b. Resolver la congruencia i 215x = 560 (mod. 2 755).
- 2, a. Resolver las congruencias de los ejercicios 1, a y 1, b por el método de la pregunta 2, c.
- b. Resolver la congruencia 1 296x m 1 105 (mód. 2 413) por el método de la pregunta 2, c.
- 3. Hallar todos los pares de números enteros x, y que satisfacen a la ecuación indeterminada 47x 111y = 89

4, a. Indicar la solución general para el sistema

$$x = b_1 \pmod{13}$$
,  $x = b_2 \pmod{17}$ .

Sirviéndose de esta solución general, hallar luego tres números que al dividirlos por 13 y 17 den los restos ) y 12, 6 y 8, 1) y 4, respectivamente.

- Indicar la solución general para el sístema
   x = b<sub>1</sub> (mód 25), x = b<sub>2</sub> (mód 27), x = b<sub>3</sub> (mód 59)
- 5, n. Resolver el sistema de congruencias (pregunta 6, n)  $x = 3 \pmod{8}$ ,  $x = 11 \pmod{20}$ ,  $x = 1 \pmod{15}$ .
- b. Resolver el sistema de congruencias

$$x = 1 \pmod{3}$$
,  $x = 4 \pmod{5}$ ,  $x = 2 \pmod{7}$ ,  $x = 9 \pmod{11}$ ,  $x = 3 \pmod{13}$ .

6. Resolver el sistema de congruencias

$$3x + 4y - 29 = 0 \pmod{143}$$
,  $2x - 9y + 84 = 0 \pmod{143}$ .

7, a. ¿A qué congruencia de grado inferior a 5 es equivalente la congruencia

$$3x^{16} + 4x^{12} + 3x^{12} + 2x^{13} + x^{0} + 2x^{0} + 4x^{7} + x^{6} + 3x^{6} + x^{6} + 4x^{6} + 2x = 0 \pmod{5}$$

b. ¿A qué congruencia de grado inferior a 7 es equivalente la congruencia

$$2x^{17} + 6x^{16} + x^{14} + 5x^{13} + 3x^{21} + 2x^{10} + x^{0} + 5x^{0} + 2x^{2} + 3x^{2} + 4x^{4} + 6x^{9} + 4x^{4} + x + 4 = 0 \pmod{7}$$

8. ¿A qué congruencia, con el coeficiente auperior igual a 1, es equivalente la congruencia (pregunta 10, a)

$$70x^6 + 78x^6 + 25x^4 + 68x^6 + 52x^6 + 4x + 3 = 0 \pmod{101}$$
?

0, a. Resolver la congruencia

$$f(z) = 0 \pmod{27}, \quad f(z) = 7z^4 + 19z + 25,$$

hallando primero mediante un tenteo todas las soluciones de la congruencia

$$f(z) = 0 \pmod{8}$$
.

b. Resolver la congruencia  $9x^2 + 29x + 62 = 0 \pmod{64}$ .

10, a. Resolver la congruencia  $x^3 + 2x + 2 = 0$  (mód. 125)

b. Resolver la congruencia  $x^4 + 4x^5 + 2x^1 + 2x + 12 = 0 \pmod{625}$ 

11, a. Resolver la congruencia  $6x^6 + 27x^6 + 17x + 20 = 0 \pmod{30}$ 

**b.** Resolver la congruencia  $31x^6 + 57x^6 + 96x + 191 = 0 \pmod{225}$ 

# CAPITULO QUINTO

# Congruencias de segundo grado

§ 1. Teoremas
 a. Entre las congruencias de grado n >
 >1, a continuación se estudiarán solamente
 las más simples, precisamente, las congruencias binómicas:

$$x^n = a \pmod{m}; (a, m) = 1. \tag{1}$$

Si la congruencia (1) admite solución, el número a se flama resto de grado n, en caso contrario, a se flama no-resto de grado n. En particular, si n=2, los restos y los no-restos se flaman cuadráticos; si n=3, cúbicos; si n=4, bicuadráticos.

b. En el presente capítulo se estudiará detalladamente el caso n=2 y, en primer lugar, las congruencias binómicas de segundo grado respecto de un módulo impar p.

$$x^{\parallel} \equiv a \pmod{p}; \quad (a, p) = 1.$$
 (2)

c. Si a es un resto cuadrático respecto del módulo p, la congruencia (2) tiene dos soluciones.

En efecto, si a es un resto cuadrático, la congruencia (2) admite al menos una solución  $x \equiv x_1 \pmod{p}$ . Pero entonces, como  $(-x_1)^3 = x_1^3$ , la misma congruencia admite también una segunda solución  $x \equiv -x_1 \pmod{p}$ . Esta segunda solución es distinta de la primera, puesto que de  $x_1 \equiv -x_1 \pmod{p}$ 

tendriamos que  $2x_1 = 0 \pmod{p}$ , lo cual es imposible, ya que  $(2, p) = (x_1, p) = 1$ .

Estas dos soluciones indicadas agotan todas las soluciones de la congruencia (2), puesto que esta última, siendo una congruencia de segundo grado, no puede admitir más de dos soluciones (c, § 4, cap IV).

d. El sistema reducido de restos respecto del módulo p consta de  $\frac{\rho-1}{2}$  restos cuadráticos, los cuales son congruen-

tes con los números

$$1^2, 2^2, \ldots, \left(\frac{\rho-1}{2}\right)^3,$$
 (3)

y de  $\frac{p-1}{2}$  no-restos cuadráticos.

En efecto, entre los restos del sistema reducido respecto del módulo p, son restos cuadráticos aquéllos, y sólo aquellos, que son congruentes con los cuadrados de los números (sistema reducido de restos)

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2},$$
 (4)

es decir, con los números (3). Por otra parte, los números (3) no son congruentes entre si respecto del módulo p, puesto que de  $k^2 = l^2 \pmod{p}$ ,  $0 < k < l < \frac{p-1}{2}$ , se deduciría, en contra de c, que a la congruencia  $x^2 = l^2 \pmod{p}$  la satisfacen cuatro de los números (4): x = -l, -k, k, l. e. Si a es un resto cuadrático respecto del módulo p, se tiene:

$$\frac{p-1}{a^{\frac{p}{3}}} = 1 \pmod{p}; \tag{5}$$

si a es un no-resto cuadrático respecto del módulo p, se tiene

$$a^{\frac{p-1}{3}} = -1 \pmod{p}$$
. (6)

En efecto, según el teorema de Fermat,

$$a^{p-1} = 1 \pmod{p}; \quad \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right) = 0 \pmod{p}.$$

Uno de los factores del primer miembro de la última congruencia, y sólo uno, es divisible por p (ambos factores no pueden simultáneamente ser divisibles por p, pues, en caso contrario, su diferencia 2 sería divisible por p). Por lo tanto, se verifica una de las congruencias (5) y (6), y sólo una

Pero todo resto cuadrático a satisface para cierto x a la congruencia

 $a = x^0 \pmod{p}$  (7)

y, por consiguiente, satisface también a la congruencia (5), la cual puede obtenerse elevando (7), término a término a la potencia  $\frac{p-1}{2}$ . Además, los restos cuadráticos agotan todas las soluciones de la congruencia (5), puesto que, siendo ésta de grado  $\frac{p-1}{2}$ , no puede tener más de  $\frac{p-1}{2}$  soluciones. Por esto, los no-restos cuadráticos satisfacen a la ecuación (6).

§ 2. Simbolo a. Introduzcamos et simbolo de Legende de Legendre de  $\left(\frac{a}{p}\right)$  (se lee así: símbolo de a con respec-

to a p). Este simbolo se define para todos los números a que no son divisibles por p, y es igual a 1, si a es un resto cuadrático, e igual a —1, si a es un no-resto cuadrático. El número a se llama numerador del simbolo y el número p, denominador del mismo.

b. En virtud de e. § 1, evidentemente, se tiene:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (\text{m\'od. } p).$$

c. Aquí deduciremos las propiedades principales del símbolo de Legendre y en el párrafo siguiente, las del símbolo de Jacobi (éste es una generalización del símbolo anterior), las cuales facilitarán el cálculo rápido de dicho símbolo, y, por consiguiente, permitirán resolver el problema de la resolubilidad de la congruencia

$$x^2 \rightleftharpoons a \pmod{p}$$
.

d. Si  $a = a_1 \pmod{p}$ , se tiene,  $\left(\frac{a}{\rho}\right) = \left(\frac{a_1}{\rho}\right)$ . Esta propiedad se debe a que los números de una misma clase son simultáneamente restos o no-restos cuadráticos.

$$e_i \left(\frac{1}{\rho}\right) = 1.$$

En efecto,  $I = I^{a}$  y, por lo tanto, I es un resto cuadrático.

$$f_{n}\left(\frac{-1}{p}\right)=\left(-1\right)^{\frac{p-1}{6}}.$$

Esta propiedad se deduce de b para a = -1.

Como  $\frac{p-1}{2}$  es par si p es de la forma 4m+1 y es impar si p es de la forma 4m+3, de aqui se deduce que -1 es un resto cuadrático respecto del módulo p, si p es de la forma 4m+1, y es un no-resto cuadrático respecto del módulo p, si p es de la forma 4m+3.

$$\mathbf{g}.\ \left(\frac{ab\dots l}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\dots\left(\frac{l}{p}\right).$$

En efecto, se tiene:

$$\left(\frac{ab \dots l}{p}\right) = \left(ab \dots l\right)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}b^{\frac{p-1}{2}} \dots l^{\frac{p-1}{2}} =$$
$$= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \dots \left(\frac{l}{p}\right) (\text{mod. } p),$$

de donde se deduce lo que se afirmaba. De aquí, como consecuencia, resulta que

$$\left(\frac{ab^3}{p}\right) = \left(\frac{a}{p}\right),$$

o sea, en el numerador del símbolo de Legendre se puede despreciar cualquier factor cuadrado.

h. Para deducir las propiedades ulteriores del símbolo de Legendre daremos primero otra interpretación del mismo. Haciendo  $p_i = \frac{p-1}{2}$ , consideremos las congruencias

donde  $e_{\pi}r_{\pi}$  es el resto absoluto mínimo de ax,  $r_{\pi}$  es su módulo de modo que  $e_{\pi} = \pm 1$ .

Los números  $a \cdot 1$ ,  $-a \cdot 1$ ,  $a \cdot 2$ ,  $-a \cdot 2$ , ...,  $a \cdot p_1$ ,  $-a \cdot p_1$  forman el sistema reducido de restos respecto del módulo p (c, § 5, cap. III); sus restos mínimos absolutos son  $\varepsilon_1 r_1$ ,  $-\varepsilon_1 r_1$ ,  $\varepsilon_2 r_2$ , ...,  $\varepsilon_{p_1} r_{p_1}$ ,  $-\varepsilon_{p_1} r_{p_2}$ . Los positivos entre estos últimos, es decir,  $r_1$ ,  $r_2$ , ...,  $r_{p_1}$ , tienen que coincidir con los números 1, 2, ...,  $p_1$  (b, § 4, cap. III).

Multiplicando ahora las congruencias (1) y simplificando por

$$1 \cdot 2 \cdot \ldots p_1 = r_1 r_2 \cdot \ldots r_{p_1}$$

obtenemos  $a^{\frac{p-1}{2}} = \varepsilon_1 \varepsilon_2 \dots \varepsilon_{p_j} \pmod{p}$ , de donde, **(b)**, se tiene

$$\left(\frac{a}{p}\right) = s_1 s_1 \dots s_{p_1}.$$
 (2)

 Demos una forma más terminada a la expresión hallada del símbolo de Legendre. Se tiene

$$\left[\frac{2ax}{p}\right] = \left[2\left[\frac{ax}{p}\right] + 2\left\{\frac{ax}{p}\right\}\right] = 2\left[\frac{ax}{p}\right] + \left[2\left\{\frac{ax}{p}\right\}\right],$$

to cual es par o impar según que el resto minimo no negativo del número ax sea menor o mayor que  $\frac{1}{2}p$ , es decir, según que sea  $\epsilon_x=1$  o  $\epsilon_x=-1$ . De aquí, evidentemente, se tiene

$$\varepsilon_z = (-1)^{\left\lceil \frac{2\alpha z}{p} \right\rceil},$$

por lo cual, de (2), hallamos;

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p}{2p+1}} \left[\frac{2ax}{p}\right].$$

J. Suponiendo a impar, transformemos la última igualdad. Se tiene (a+p) es par)

$$\left(\frac{2a}{\rho}\right) = \left(\frac{2a+2p}{\rho}\right) = \left(\frac{4\frac{a+p}{2}}{\rho}\right) = \left(\frac{a+\rho}{2}\right) = \left(\frac{$$

de donde

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{m=1}^{p_1} \left[\frac{a_m}{p}\right] + \frac{p_3 - 1}{3}}$$
. (3)

La fórmula (3) nos permitirá deducir dos propiedades muy importantes del simbolo de Legendre.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{6}}.$$

Es consecuencia de la fórmula (3) para a=1. Pero p puede expresarse en la forma p=8m+s, donde s es uno de los números 1, 3, 5, 7. Además  $\frac{p^2-1}{8}=8m^2++2ms+\frac{s^2-1}{8}$ , siendo este número par si s=1 ó s=7 e impar si s=3 ó s=5. Por lo tanto, el número 2 es un resto cuadrático respecto del módulo p si p es de la forma 8m+1 o de la forma 8m+7 y es un no-resto cuadrático respecto del módulo p si p es de la forma 8m+3 o de la forma 8m+5.  Si p y q son primos impares, se tiene (ley reciproca de los restos cuadráticos).

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Como  $\frac{p-1}{2}$ ,  $\frac{q-1}{1}$  es impar solamente cuando ambos números p y q son de la forma 4m+3, y es par si al menos uno de estos números es de la forma 4m+1, la propiedad señalada se puede formular asi:

Si ambos números p y q son de la forma 4m + 3, se tiene:

$$\left(\frac{q}{p}\right) - \left(\frac{p}{q}\right);$$

si al menos uno de ellos es de la forma 4m -1, se tiene:

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$
,

Para llevar a cabo la demostración, obsérvese que, en virtud de K, la fórmula (3) foma la forma

$$\left(\frac{a}{p}\right) - \left(-1\right)^{\frac{n}{n-1}\left\{\frac{au}{p}\right\}}.$$
(4)

Haciendo ahora  $\frac{q-1}{2} \sim q_1$ , consideremos los  $p_1q_1$  pares de números que se obtienen cuando en las expresiones qx, py los números x e y recorren, independientemente uno del otro, los sistemas de valores

$$x = 1, 2, \ldots, p_t, y = 1, 2, \ldots, q_t$$

Nunca puede ocurrir que sea qx = py, puesto que de esta igualdad se deduciría que py es múltiplo de q, lo cual es imposible, puesto que (p, q) = (y, q) - 1 (ya que 0 < y < q). Por lo tanto, se puede hacer  $p_1q_1 = S_1 + S_2$ , donde  $S_1$  es el número de pares con qx < py y  $S_2$  es el número de pares con py < qx.

Evidentemente,  $S_1$  es también el número de pares con  $x < \frac{p}{q}y$ . Aquí, para cada y dado se puede tomar x = 1,  $2, \ldots, \left[\frac{p}{q}y\right]$  (Como  $\frac{p}{q}y \leqslant \frac{p}{q}q_1 < \frac{p}{2}$ , se tiene  $\left[\frac{p}{q}y\right] \leqslant \leqslant p_1$ ). Por consiguiente,

$$S_1 = \sum_{\nu=1}^{q_1} \left[ \frac{\rho}{q} y \right].$$

De un modo análogo, nos convencemos de que

$$S_3 = \sum_{x=1}^{p_1} \left[ \frac{q}{p} x \right].$$

Pero entonces, según la igualdad (4), se tiene

$$\left(\frac{p}{q}\right) = (-1)^{8_1}, \quad \left(\frac{q}{p}\right) = (-1)^{8_1},$$

por lo cual,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{S_1+S_2}-\left(-1\right)^{p_1q_1},$$

de donde se deduce la propiedad indicada.

§ 3. Simbolo a. Para conseguir mayor rapidez en el de Jacobi cálculo del símbolo de Legendre, se considera el simbolo más general de Jacobi. Sea P impar, mayor que la unidad, y sea  $P = p_1p_2 \dots p_r$ , su descomposición en factores primos (entre ellos también puede haber iguales). Supongamos también que (a, P) = 1. Entonces el símbolo de Jacobi  $\left(\frac{a}{P}\right)$  se define por la igualdad  $^1$ )

$$\left(\frac{a}{P}\right) = \left(\frac{a}{\rho_1}\right)\left(\frac{a}{\rho_2}\right) \dots \left(\frac{a}{\rho_r}\right).$$

<sup>1)</sup> En el segundo miembro,  $\left(\frac{a}{\rho_d}\right)$  denota el simbolo de Legendre. Por lo tanto, para P primo, los símbolos de Jacobi y de Legendre coinciden  $(N, del T_i)$ .

Las propiedades conocidas del símbolo de Legendre permiten establecer las propiedades análogas para el símbolo de Jacobí.

b. Si  $a = a_i \pmod{P}$ , se tiene  $\left(\frac{a}{P}\right) = \left(\frac{a_i}{P}\right)$ . En efecto.

$$\left(\frac{a}{P}\right) = \left(\frac{a}{\rho_1}\right)\left(\frac{a}{\rho_2}\right) \dots \left(\frac{a}{\rho_r}\right) = \left(\frac{a_1}{\rho_1}\right)\left(\frac{a_1}{\rho_2}\right) \dots \left(\frac{a_1}{\rho_r}\right) = \left(\frac{a_1}{P}\right),$$

puesto que a, siendo congruente con  $a_1$  respecto del módulo P, es también congruente con  $a_1$  respecto de los módulos  $p_1$ ,  $p_2$ , . . . ,  $p_r$ , ya que éstos son divisores de P.

c. 
$$\left(\frac{1}{P}\right) = 1$$
.

En efecto,

$$\left(\frac{1}{p}\right) = \left(\frac{1}{p_1}\right)\left(\frac{1}{p_4}\right) \ldots \left(\frac{1}{p_r}\right) \Rightarrow 1.$$

**d.** 
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$
.

Para demostrar esto, obsérvese que

$$\left(\frac{-1}{p}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right) \dots \left(\frac{-1}{p_r}\right) \Rightarrow$$

$$= \left(\frac{p_1-1}{2} + \frac{p_2-1}{2} + \dots + \frac{p_r-1}{2}\right); \qquad (1)$$

pero

$$\frac{p-1}{2} = \frac{p_1p_1 \dots p_r-1}{2} =$$

$$= \frac{\left(1+2\frac{p_1-1}{2}\right)\left(1+2\frac{p_3-1}{2}\right) \dots \left(1+2\frac{p_r-1}{2}\right) -1}{2} = \frac{p_3-1}{2} + \frac{p_3-1}{2} + \dots + \frac{p_r-1}{2} + 2N,$$

en virtud de lo cual, de la fórmula (1) deducimos que

$$\left(\frac{-1}{P}\right) = \left(-1\right)^{\frac{P-1}{2}}.$$

$$\mathbf{e}.\left(\frac{ab\ldots l}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\ldots\left(\frac{l}{p}\right).$$

En efecto,

reuniendo los símbolos que tienen iguales numeradores, se obtiene la propiedad en cuestión. De aquí resulta la consecuencia

$$\left(\frac{ab^2}{P}\right) = \left(\frac{a}{P}\right)$$
.

$$\mathbb{I}_* \left( \frac{2}{P} \right) = (-1)^{\frac{P!-1}{6}}.$$

En efecto,

$$\left(\frac{2}{p}\right) = \left(\frac{2}{p_1}\right) \left(\frac{2}{p_2}\right) \dots \left(\frac{2}{p_r}\right) = \frac{p_1^{\delta-1} + p_1^{\delta-1}}{\delta} + \dots + \frac{p_r^{\delta-1}}{\delta},$$
(2)

Pero

$$\frac{P^{2}-1}{8} = \frac{p[p] \dots p[-1]}{8} = \frac{\left(1+8\frac{p[-1]}{8}\right)\left(1+8\frac{p[-1]}{8}\right)\dots\left(1+8\frac{p[-1]}{8}\right)-1}{8} = \frac{p[-1]}{8} + \frac{p[-1]}{8} + \dots + \frac{p[-1]}{8} + 2N,$$

en virtud de lo cual, de la fórmula (2) deducimos que

$$\left(\frac{2}{P}\right) = \left(-1\right)^{\frac{P^2-1}{6}}.$$

g. Si P y Q son números impares positivos, primos entre si, se tiene

$$\left(\frac{Q}{P}\right) = \left(-1\right)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \left(\frac{P}{Q}\right).$$

En efecto, supongamos que  $Q = q_1q_2 \dots q_n$  es la descomposición de Q en factores primos (entre éstos, de nuevo puede haber iguales). Se tiene

$$\frac{\left(\frac{Q}{P}\right) - \left(\frac{Q}{p_1}\right) \left(\frac{Q}{p_2}\right) \cdots \left(\frac{Q}{p_r}\right) = \prod_{\alpha=1}^r \prod_{\beta=1}^d \left(\frac{q_\beta}{p_\alpha}\right) = \\
- \left(-1\right)^{\alpha-1} \prod_{\beta=1}^r \frac{\sum_{\alpha=1}^d \frac{p_\alpha-1}{2}}{2} \prod_{\alpha=1}^r \prod_{\beta=1}^d \left(\frac{p_\alpha}{q_\beta}\right) = \\
- \left(-1\right)^{\left(\sum_{\alpha=1}^r \frac{p_\alpha-1}{2}\right)} \left(\sum_{\beta=1}^s \frac{q_\beta-1}{2}\right) \left(\frac{p}{Q}\right).$$

Pero, de un modo semejante a lo que se hizo en d, hallamos

$$\frac{P-1}{2} = \sum_{\alpha=1}^{r} \frac{p_{\alpha}-1}{2} + 2N, \quad \frac{Q-1}{2} = \sum_{\beta=1}^{0} \frac{q_{\beta}-1}{2} + 2N_{1},$$

en virtud de lo cual, la última fórmula implica que

$$\left(\frac{Q}{P}\right) = \left(-1\right)^{\frac{P-1}{2} \cdot \frac{Q-1}{2}} \left(\frac{P}{Q}\right).$$

Ejemplo. Como un ejemplo de cálculo del símbolo de Legendre (además, a éste lo vamos a considerar como un caso particular del símbolo de Jacobi) averiguemos si admite solución la congruencia

$$x^3 = 219 \pmod{.383}$$
.

Se tiene (aplicando sucesivamente las propiedades g, b, la consecuencia e, g, b, e, f, g, b, d):

por lo tanto, la congruencia considerada tiene dos soluciones.

§ 4. Caso de un módulo compuesto a. Las congruencias de segundo grado respecto de un módulo compuesto se estudian y resuelven de acuerdo a las indi-

caciones del 6 5, cap. IV.

b. Comencemos con las congruencias de la forma

$$x^{a} \equiv a \pmod{p^{a}}; \ \alpha > 0, \ (a, p) = 1,$$
 (1)

donde p es un número primo Impar.

Haciendo  $f(x) = x^{0} - a$ , se tiene f'(x) = 2x, y si  $x = x_{1} \pmod{p}$  es una solución de la congruencia

$$x^3 = a \pmod{p},$$
 (2)

entonces, en virtud de que (a, p) = 1 también  $(x_1, p) = 1$ , y como p es impar, resulta  $(2x_1, p) = 1$ , es decir,  $f'(x_1)$  no es divisible por p. Por lo tanto, para la búsqueda de las soluciones de la congruencia (1) se pueden aplicar los razonamientos b, § 5, cap IV, proporcionando cada solución de la congruencia (2) una solución de la congruencia (1). De lo expuesto deducimos que:

La congruencia (1) tiene dos soluciones o ninguna, según que el número a sea un resto cuadrático o un no-resto cuadrático respecto del módulo p.

c. Consideremos ahora la congruencia

$$x^a \equiv a \pmod{2^a}; \quad \alpha > 0, \quad (a, 2) = 1.$$
 (3)

En este caso  $f'(x_i) = 2x_i$  es divisible por 2, por lo cual no pueden aplicarse los razonamientos expuestos en b, § 5, cap IV; éstos deben modificarse del modo siguiente: d. Si la congruencia (3) admite solución, entonces, como

d. Si la congruencia (3) admite solución, entonces, como (a, 2) = 1, se tiene (x, 2) = 1; por consiguiente  $(k, \S 2)$ ,  $x^3 - 1$  es divisible por 8 Por esta razón, reduciendo la congruencia (3) a la forma

$$(x^3 - 1) + 1 = a \pmod{2^a}$$
.

nos convencemos de que para que esta congruencia admita solución es necesario que sea

$$a = 1 \pmod{4}$$
 si  $\alpha = 2$ ;  $a = 1 \pmod{8}$  si  $\alpha \geqslant 3$ . (4)

 e. Supongamos cumplidas las condiciones (4), examinemos el problema de la búsqueda de las soluciones y de la cantidad de ellas.

En virtud de d, en los casos en que  $\alpha \leqslant 3$ , a la congruencia satisfacen todos los números impares. Por lo tanto, la congruencia  $x^a \equiv a \pmod{2}$  tiene una solución:  $x \equiv 1 \pmod{2}$  la congruencia  $x^a \equiv a \pmod{4}$  tiene dos soluciones:  $x \equiv 1$ ; 3 (mód. 4), la congruencia  $x^a \equiv a \pmod{8}$  tiene cuatro soluciones:  $x \equiv 1$ ; 3, 5; 7 (mód. 8).

Para examinar los casos  $\alpha = 4, 5, \dots$  es convergente reunir todos los números impares en dos progresiones aritméticas:

$$x = \pm (1 + 4t_3) \tag{5}$$

$$(1 + 4t_3 \equiv 1 \pmod{4}; -1 - 4t_3 \equiv -1 \equiv 3 \pmod{4}).$$

Veamos cuáles de los números (5) satisfacen a la congruencia  $x^3 = a \pmod{16}$ . Obtenemos

$$(1+4t_3)^3 = a \pmod{16}, \quad t_3 = \frac{a-1}{8} \pmod{2},$$
  
 $t_3 = t_1' + 2t_4, \quad x = \pm (1+4t_2' + 8t_4) = \pm (x_4 + 8t_4).$ 

Veamos cuáles de los últimos números satisfacen a la congruencia  $x^a \equiv a \pmod{32}$ . Obtenemos

$$(x_4 + 8t_4)^2 = a \pmod{32}, \quad t_4 = t'_4 + 2t_5, x = \pm (x_4 + 16t_5),$$

etc. De este modo, demostramos que para cualquier  $\alpha > 3$  los valores x que satisfacen a la congruencia (3) se expresan en la forma

$$x = \pm (x_\alpha + 2^{\alpha - 1}t_\alpha).$$

Estos valores x forman cuatro soluciones distintas de la congruencia (3)

$$x = x_{\alpha}, \quad x_{\alpha} + 2^{\alpha - 1}; \quad -x_{\alpha}; \quad -x_{\alpha} = 2^{\alpha - 1} \pmod{2^{\alpha}}$$

(respecto del módulo 4, las dos primeras son congruentes con 1 y las dos últimas con -1)

Ejemplo. La congruencia

$$x^3 = 57 \text{ (mód. 64)}$$
 (6)

admite cuatro soluciones, puesto que  $57 \equiv 1 \pmod{8}$ . Expresando x en la forma  $x = \pm (1 + 4t_3)$ , obtenemos

$$(1 + 4t_3)^n \equiv 57 \pmod{16}, 8t_3 \equiv 56 \pmod{16},$$
 $t_3 \equiv 1 \pmod{2}, t_2 = 1 + 2t_4, x = \pm (5 + 8t_4),$ 
 $(5 + 8t_4)^n = 57 \pmod{32}, 5 \cdot 16t_4 \equiv 32 \pmod{32},$ 
 $t_4 \equiv 0 \pmod{2}, t_4 = 2t_6, x = \pm (5 + 16t_6),$ 
 $(5 + 16t_6)^n \equiv 57 \pmod{64}, 5 \cdot 32t_6 \equiv 32 \pmod{64},$ 
 $t_5 \equiv 1 \pmod{2}, t_6 = 1 + 2t_6, x = \pm (21 + 32t_6).$ 

Por lo tanto, las soluciones de la congruencia (6) son:

$$x = \pm 21$$
;  $\pm 53$  (mód. 64).

I. De c, d y e se deduce que:

Para la congruencia

$$x^a = a \pmod{2^a}$$
;  $(a, 2) = 1$ 

las condiciones necesarias de resolubilidad son:  $a \equiv 1 \pmod{4}$  si  $\alpha = 2$ ,  $a \equiv 1 \pmod{8}$  si  $\alpha \geqslant 3$ . Si se cumplen estas condiciones, el número de soluciones es igual a: 1 si  $\alpha = 1$ ; 2 si  $\alpha = 2$ ; 4 si  $\alpha \geqslant 3$ .

g. De b, f y a, § 5. cap IV se deduce que

Para la congruencia de la forma general

$$x^{\mathbf{k}} = a \pmod{m}; \quad m = 2^{\alpha} \rho_1^{\alpha_1} \rho_2^{\alpha_k} \dots \rho_k^{\alpha_k}; \quad (a, m) = 1$$

las condiciones necesarias de resolubilidad son:

$$a = 1 \pmod{4}$$
 si  $\alpha = 2$ ,  $a = 1 \pmod{8}$  si  $\alpha \ge 3$ ,  $\left(\frac{a}{p_1}\right) = 1$ ,  $\left(\frac{a}{p_2}\right) = 1$ , ...,  $\left(\frac{a}{p_k}\right) = 1$ .

St se cumplen todas estas condiciones, el número de soluciones es igual a:  $2^h$  st  $\alpha = 0$  y si  $\alpha = 1$ ;  $2^{h+1}$  st  $\alpha = 2$ ;  $2^{h+2}$  st  $\alpha \geqslant 3$ .

# Preguntas referentes al capitulo V

A continuación, la letra p denotará siempre un número primo ітраг.

1. Demostrar que la búsqueda de las soluciones de una congruencia de la forma

$$ax^{2} + bx + c = 0 \pmod{m}$$
,  $(2a, m) = 1$ ,

se reduce a la búsqueda de las soluciones de una congruencia de la forma  $x^2 \equiv a \pmod{m}$ .

2. a. Aplicando e, § 1, hallar las soluciones de la congruencia (en caso de que ello sea posible)

$$x^2 \equiv a \pmod{p}$$
;  $p = 4m + 3$ 

b. Aplicando b y k, § 2, indicar un método para buscar las soluciones de las congruencias de la forma

$$x^{s} \approx a \pmod{p}$$
;  $p = 8m + 5$ .

c. Indicar el método más sencillo posible para buscar las soluciones de las congruencias de la forma

$$x^a \equiv a \pmod{p}$$
;  $p = 8m + 1$ ,

si se conoce un número N que es un no-resto cuadrático respecto del módulo p.

d. Aplicando el teorema de Wilson, demostrar que las soluciones de la congruencia

$$x^2 + 1 = 0 \text{ (mod. p)}; \quad p = 4m + 1$$

son

$$x = \pm 1 \cdot 2 \dots 2m \pmod{p}$$
.

3. a. Demostrar que la congruencia

$$x^n + 1 = 0 \pmod{p} \tag{1}$$

admite solución cuando, y sólo cuando, p es de la forma 4m + 1; la congruencia

$$x^2 + 2 \equiv 0 \text{ (mod. p)} \tag{2}$$

admite solución cuando, y sólo cuando, p, es de la forma 8m + 1 ó 8m + 3; la congruencia

$$x^0 + 3 \equiv 0 \pmod{p} \tag{3}$$

admite solución cuando, y sólo cuando, p es de la forma 6m + 1.

- b. Demostrar que la cantidad de números primos de la forma 4m + 1 es infinita.
- c. Demostrar que la cantidad de números primos de la forma 6m + 1 es infinits.
- 4. Supongamos que, dividiendo a los números 1, 2, . . ., p-1 en dos conjuntos, de modo que el segundo contenga al menos un número, se tiene:
- el producto de dos números de un conjunto es congruente respecto del módulo p con un número del primer conjunto, mientras que el producto de dos números de distintos conjuntos es congruente respecto del módulo p con un número del segundo conjunto. Demostrar que esto ocurre cuando, y sólo cuando, el primer conjunto consta de los restos cuadráticos y el segundo, de los no-restos cuadráticos respecto del módulo p.
- a. Deducir la teoría de las congruencias de la forma
   x<sup>a</sup> ≡ a (mód. p<sup>a</sup>): (a, p) = 1.

expresando a y x en el sistema de numeración de base p.

b. Deducir la teoria de las congruencias de la forma

$$x^{n}$$
 and  $a$  (mod.  $2^{n}$ );  $(a, 2) = 1$ ,

expresando a y x en el sistema de numeración de base 2.

6. Demostrar que las soluciones de la congruencia

$$x^{0} \equiv a \pmod{p^{0}}; (a, p) = 1,$$

son  $x = \pm PQ'$  (mód.  $p^n$ ), donde

$$P = \frac{(z + \sqrt{a})^{\alpha} + (z - \sqrt{a})^{\alpha}}{2}, \quad Q = \frac{(z + \sqrt{a})^{\alpha} - (z - \sqrt{a})^{\alpha}}{2\sqrt{a}},$$
$$z^{2} = a \text{ (mod. } p), \quad QQ' = 1 \text{ (mod. } p^{\alpha})$$

7. Indicar un método de resolución de la congruencia  $x^2 = 1 \pmod{m}$ , que se base en la circunstancia de que la congruencia expuesta es equivalente a la siguiente:  $(x-1)(x+1) = 0 \pmod{m}$ .

**8.** Sea 
$$\left(\frac{a}{p}\right) = 0$$
 si  $(a, p) = p$ .

a. Siendo (k, p) = 1, demostrar que

$$\sum_{n=0}^{p-1} \left( \frac{x(x+h)}{p} \right) = -1.$$

b. Supongamos que cada uno de los números  $\varepsilon$  y  $\eta$  tiene uno de los valores  $\pm$  1. T es la cantidad de pares x, x + 1, con la condición  $\left(\frac{x}{p}\right) = \varepsilon$ ,  $\left(\frac{x+1}{p}\right) = \eta$ , donde  $x = 1, 2, \ldots$  p-2. Demostrar que

$$T = \frac{1}{4} \left( \rho - 2 - \varepsilon \left( \frac{-1}{\rho} \right) - \eta - \varepsilon \eta \right).$$

c. Supongamos que (k, p) = 1,

$$S = \sum_{x} \sum_{y} \left( \frac{xy + h}{p} \right).$$

donde x e y recorren las sucesiones crecientes, formadas por X e Y restos, respectivamente, del sistema completo respecto del módulo p. Demostrar que

$$|S| < V \overline{XYp}$$
.

Para la demostración se debe aplicar la desigualdad 1)

$$S^2 \leqslant X \sum_{\pi} \left| \sum_{y} \left( \frac{xy + h}{p} \right) \right|^2$$

$$\left(\sum_{k=1}^{n} x_{k}\right)^{2} < n \sum_{k=1}^{n} x_{k}^{2}.$$

(N. del T.).

<sup>1)</sup> Esta desigualdad se obtiene aplicando la desigualdad bien conocida:

d. Sea Q entero, 1 < Q < p,

$$S = \sum_{x=0}^{p-1} S_x^a; \ S_x = \sum_{k=0}^{Q-1} \left(\frac{x+z}{p}\right).$$

- a) Demostrar que  $S = (\rho Q) Q$
- β) Sea λ constante;  $0 < \lambda < 1$ . Demostrar que la cantidad T de números de la sucesión  $x = 0, 1, \ldots, p-1$ , para los cuales no se cumple la condición  $S_x \le Q^{0.5+0.5\lambda}$ , satisface a la condición  $T \le pQ^{-\lambda}$ .
- y) Sea M entero,  $Q = \{\sqrt{\rho}\}, 0 < M, M + 2Q \le \rho$ . Demostrar que en la sucesión

$$M, M + 1, \ldots, M + 2Q - 1$$

hay un no-resto cuadrático respecto del módulo p.

 $\theta$ , a. Demostrar que el número de expresiones de un entero m > 1 en la forma

$$m = x^3 + y^3$$
,  $(x, y) = 1$ ,  $x > 0$ ,  $y > 0$  (1)

es igual al número de soluciones de la congruencia

$$z^2 + 1 = 0 \text{ (mod. } m). \tag{2}$$

Para la demostración, hacer  $\tau = \sqrt{m}$ , utilizar la expresión de  $\alpha = \frac{z}{m}$  según el teorema de la pregunta 4, b, cap. I, y considerar la congruencia que se obtiene al multiplicar término a término (2) por  $Q^2$ .

b. Sea a uno de los números 2 y 3. Demostrar que el número de expresiones de un número primo p, con la condición p > a, en la forma

$$p = x^a + ay^a, \quad x > 0, \quad y > 0,$$
 (3)

es igual a la mitad del número de soluciones de la congruencia

$$z^{a} + a \equiv 0 \text{ (mod. } p). \tag{4}$$

c. Sea p de la forma 4m + 1, (k, p) = 1,

$$S(k) = \sum_{x=0}^{p-1} \left( \frac{x(x^2+k)}{p} \right).$$

Demostrar que

a) 5(k) es un número par.

$$\beta) S(kt^{k}) = \left(\frac{t}{\rho}\right) S(k).$$

 $\gamma$ ) Si  $\left(\frac{r}{\rho}\right) = 1$ ,  $\left(\frac{n}{\rho}\right) = -1$ , se tiene (compárese con la pregunta a)

 $p = \left(\frac{1}{2}S(r)\right)^2 + \left(\frac{1}{2}S(n)\right)^3$ 

10. Sea D un entero positivo que no sea el cuadrado de un número entero. Demostrar que:

a. Si para un entero dado k, satisfacen a la ecuación

$$x^a - Dy^a = k$$

dos pares de números enteros  $x=x_1$ ,  $y=y_1$  y  $x=x_2$ ,  $y=y_2$ , entonces a la ecuación

$$X^a - DY^a = k^a$$

satisfacen los números enteros X, Y que se determinan por la igualdad (el signo  $\pm$  se elige arbitrarlamente)

$$X + Y \sqrt{\overline{D}} = (x_1 + y_1 \sqrt{\overline{D}}) (x_2 \pm y_2 \sqrt{\overline{D}}).$$

b. La ecuación (ecuación de Pell)

$$x^{0} \leftarrow Du^{0} = 1 \tag{1}$$

es resoluble en números enteros positivos x, y.

c. Si  $x_0$ ,  $y_0$  es el par de números positivos x, y con el valor menor de x (o, lo que es equivalente, con el valor menor de  $x + y | \nabla \overline{D}$ ), que satisface a la ecuación (1), entonces todos los pares de números positivos x, y que satisfacen a esta ecuación, se determinan por la igualdad

$$x + y \sqrt{D} = (x_0 + y_0 \sqrt{D})^r; \quad r = 1, 2, \dots$$
 (2)

a. Sea α υπ número entero.

$$U_{a,p} = \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i \frac{dx}{p}}.$$

a) Siendo (a, p) = 1, demostrar que  $\|U_{a, p}\| = \sqrt{p}$ Para la demostración, se debe multiplicar la suma  $U_{a, p}$  por la conjugada que se obtiene al sustituir i por -i. Designando con las letras  $x_i$  y x las variables de sumación de la suma fundamental y de la conjugada, respectivamente, se deben reunir aquellos términos del producto en los que para un t dado

$$x_1 = xt \pmod{p}$$
,

o bien

$$x_1 \equiv x + t \pmod{p}$$
.

β) Demostrar que

$$\left(\frac{a}{p}\right) = \frac{U_{a,p}}{U_{1,p}}$$
.

b. Sea m > 2, (a, m) = 1,

$$S_{a, m} = \sum_{m=1}^{m-1} e^{2\pi i \frac{a x^2}{m}},$$

a) Demostrar que  $S_{a,p} = U_{a,p}$  (pregunta a).

β) De los teoremas de las preguntas α) y a, α) se deduce que  $|S_a, p| = V \overline{p}$ . Demostrar el siguiente aserto más general:

$$|S_{a,m}| = \sqrt{m}$$
, si  $m = 1 \pmod{2}$ ,  $|S_{a,m}| = 0$ , si  $m = 2 \pmod{4}$ ,  $|S_{a,m}| = \sqrt{2m}$ , si  $m = 0 \pmod{4}$ .

y) Sea m > 1, (2A, m) = 1, a = cualquier número entero.Demostrar que

$$\big|\sum_{n=0}^{m-1}e^{2\pi i\frac{Ax^2+ax}{m}}\big|=\sqrt{m}.$$

12, a. Supongamos que m es un número entero, superior a 1, z recorre Z números enteros dados,  $\sum_{x}$  denota una suma extendida a todos estos números

 $\alpha$ ) Sea ia función  $\Phi(x)$  tal, que para cualquier  $a=1, 2, \ldots, m-1$  se tiene

$$\big|\sum_{z}\Phi\left(z\right)e^{\frac{2\pi i}{m}}\big|\ll\Delta.$$

Supongamos también que M y Q son enteros, 0 < M < M + 1 Q < m, y que  $\sum_{z}^{r}$  denota una suma extendida solamente a aquellos valores de z que son congruentes con los números de la sucesión M, M+1, ..., M+Q-1 respecto del módulo m. Demostrar que

$$\sum_{z}' \Phi(z) = \frac{Q}{m} \sum_{z} \Phi(z) + \theta \Delta (\ln m - \delta),$$

donde  $|\theta| < 1$ ,  $\delta > 0$  siempre,  $\delta > 0.5$  si m > 12.  $\delta > 1$  si m > 60.

β) Supongamos que para cualquier a = 1, 2, ..., m-1 se tiene

$$\left|\sum_{x}e^{2\pi i \cdot \frac{\Delta x}{m}}\right| < \Delta_0$$

y sea N un número entero arbitrario. Entonces, para

$$l = \left[ \frac{2\Delta_0 m}{2} \right]$$

existe al menos un valor z que es congruente con uno de los números de la sucesión

$$N-1, \ldots, N-1, N, N+1, \ldots, N+l$$

respecto del módulo m.

b. Sean M y Q enteros,  $0 < M < M + Q \le p$ .

a). Demostrar que

$$\Big|\sum_{n=M}^{M+Q-1} \left(\frac{x}{p}\right)\Big| < V \hat{p} \ln p.$$

β) Sea R el número de restos cuadráticos y N el número de no-restos cuadráticos en la sucesión M, M+1, ...

..., M+Q-1. Demostrar que

$$R = \frac{1}{2} Q + \frac{\theta}{2} \sqrt[p]{p} \ln p, \quad N = \frac{1}{2} Q - \frac{\theta}{2} \sqrt[p]{p} \ln p; \mid \theta \mid < 1.$$

- γ) Deducir la fórmula de la pregunta β) aplicando el teorema de la pregunta 11, b, β) y el teorema de la pregunta a.
- 8) Sea (2A, m) = 1,  $M_0$  y  $Q_0$  son enteros,  $0 < M_0 < M_0 + Q_0 \le m$ . Demostrar que para  $m \ge 60$

$$|\sum_{x=M_0}^{M_0+Q_0-1} e^{2\pi i \frac{Ax^3}{m}}| < \sqrt{m} \ln m.$$

r) Supongamos que  $(A, \rho) = 1$ ,  $M_0$  y  $Q_0$  son enteros,  $0 < M_0 < M_0 + Q_0 < \rho$  y T denota la cantidad de números de la sucesión  $Ax^2$ ,  $x = M_0$ ,  $M_0 + 1$ , ...,  $M_0 + Q_0 - 1$ , que son congruentes con los números de la sucesión M, M+1, ..., M+Q-1 respecto del módulo  $\rho$ . Demostrar que para  $m \gg 60$ 

$$T = \frac{Q_0 Q}{p} + \theta \sqrt{p} (\ln p)^2.$$

 c. Deducir las fórmulas de la pregunta b, β) examinando la suma

$$\sum_{n=1}^{p-1}\sum_{\alpha=1}^{p-1}\sum_{x=M}^{M+Q-1}\sum_{\nu=M}^{M+Q-1}\left(\frac{\alpha}{\rho}\right)e^{2\pi i\frac{\alpha(x-\alpha\nu)}{p}}$$

#### Ejercicios numéricos referentes al capitalo V

- a. Señálense los restos cuadráticos entre los restos del sistema reducido respecto del módulo 23.
- Señálense los no-restos cuadráticos entre los restos del sistema reducido respecto del módulo 37
- 2, a. Aplicando e, § 1, Indicar el número de soluciones de las con gruencias
  - (a)  $x^0 = 3 \pmod{31}$ ; (b)  $x^0 = 2 \pmod{31}$
- b. Indicar el número de soluciones de las congruencias
  - a)  $x^0 = 5 \pmod{73}$ ; b)  $x^0 = 3 \pmod{73}$

- 8, a. Calculando el símbolo de Jacobi, indicar el número de soluciones de las congruencias
  - $\alpha$ )  $x^3 = 226 \pmod{563}$ ;  $\beta$ )  $x^4 = 429 \pmod{563}$
- Indicar el número de soluciones de las congruencias
  - $\alpha$ )  $x^3 = 3.766$  (mód. 5.987);  $\beta$ )  $x^3 = 3.149$  (mód. 5.987).
- 4, a. Aplicando los métodos de las preguntas 2, a; 2, b;2, c resolver las congruencias
- (a)  $x^2 = 5 \pmod{19}$ ; (b)  $x^3 = 5 \pmod{29}$ ; (c)  $x^4 = 2 \pmod{97}$
- b. Resolver has congruencias
- (a)  $x^2 = 2 \pmod{3!1}$ , (b)  $x^3 = 3 \pmod{277}$ ; (c)  $x^4 = 11 \pmod{353}$ .
- 5, a. Resolver la congruencia  $x^9 = 59 \pmod{125}$  aplicando los métodos:
- α) b, § 4, β) de la pregunta 5, a; γ) de la pregunta 6.
- b. Resolver la congruencia x<sup>2</sup> = 91 (mód. 243).
- 8, n. Resolver la congruencia x<sup>3</sup> = 41 (mód. 64) aplicando los métodos
- α) e, 6 4, β) de la pregunta 5, b.
- b. Resolver is congruencia x = 145 (mod 256)

## CAPITULO SEXTO

# Raíces primitivas e índices

§ 1. Teoremas a. Si (a, m) = 1, existen enteros positivos  $\gamma$  con la condición  $a^{\gamma} = 1$  (mód m), por ejemplo (según el teorema de Euler),  $\gamma = \varphi$  (m). El menor de ellos se llama exponente, al cual pertenece el número a respecto del módulo m.

b. Si a pertenece al exponente  $\delta$  respecto del módulo m, los números  $1 = a^0$ ,  $a^1$ , ...,  $a^{b-1}$  no son congruentes entre si

respecto del módulo m.

En efecto, si fuese  $a^t = a^k \pmod{m}$ ,  $0 \le k < t < \delta$  resultaría que  $a^{t-k} = 1 \pmod{m}$ , siendo  $0 < t - k < \delta$ , lo cual contradice a la definición de  $\delta$ .

c. Si a pertenece al exponente  $\delta$  respecto del módulo m, entonces  $a^{\gamma} \equiv a^{\gamma'}$  (mód. m) cuando, y sólo cuando,  $\gamma = \gamma'$  (mód.  $\delta$ ); en particular (si  $\gamma' = 0$ ),  $a^{\gamma} = 1$  (mód. m) cuando, y sólo cuando,  $\gamma$  es divisible por  $\delta$ .

En efecto, sean r y  $r_1$  los restos no negativos mínimos de los números  $\gamma$  y  $\gamma'$  respecto del módulo  $\delta$ ; entonces, para ciertos enteros q y  $q_1$ , se tiene  $\gamma = \delta q + r$ ,  $\gamma' = \delta q_1 + r_1$ . De aquí, en virtud de que  $a^{\delta} \equiv 1 \pmod{m}$ , resulta que

$$a^{\gamma} = (a^0)^q a^r = a^r \pmod{m},$$
  
 $a^{\gamma'} = (a^0)^{q_1} a^{r_1} = a^{r_2} \pmod{m}.$ 

Por lo tanto,  $a^{r} = a^{r_1} \pmod{m}$  cuando, y sólo cuando,  $a^{r} = a^{r_1} \pmod{m}$ , es decir, (b), cuando  $r = r_i$ .

d. Como  $a^{\varphi(m)} \equiv 1 \pmod{m}$ , de c (y' = 0) se deduce que φ (m) es divisible por δ. Por consiguiente, los exponentes a los cuales pertenecen los números respecto del módulo m. son divisores de  $\varphi$  (m). El mayor entre estos divisores es el mismo número  $\phi$  (m). Los números que pertenecen al exponente  $\phi$  (m) (si tales existen) se llaman raices primitivas respecto del módulo m.

8 2. Raices primitioas respecto de tos módutos na y 2pa

 Sea ρ un número primo impar y α > 1. Demostremos la existencia de raíces primitivas respecto de los módulos pa y 2pa. b. Si x pertenece al exponente ab respecto del módulo m, entonces xª pertenece al exponente b.

En efecto, supongamos que xª pertenece al exponente ô. Entonces  $(x^{ab}) \equiv 1 \pmod{m}$ , de donde  $x^{ab} \equiv 1 \pmod{m}$ ; por lo tanto (c. 8 1), aô es divisible por ab, es decir, ô es divisible por b Por otra parte, xab = 1 (mod. m), de donde  $(x^a)^b = 1 \pmod{m}$ ; por consigniente (c. § 1), b es divisible por  $\delta$ . Por lo tanto,  $\delta = b$ .

c. Si x pertenece al exponente a e y pertenece al exponente b respecto del módulo m, u (a, b) : 1, entonces xu pertenece al exponente ab.

En efecto, supongamos que xu pertenece al exponente ô. Entonces  $(xy)^b = 1 \pmod{m}$ . De aqui resulta que  $x^{bb} y^{bb} =$  $= 1 \pmod{m}$  y (c, § 1)  $x^{66} = 1 \pmod{m}$ . Por lo tanto (c, § 1),  $b\delta$  es divisible por a, y como (b, a) = 1,  $\delta$  es divisible por a. Del mismo modo hallamos que 8 es divisible por b. El número δ, siendo divisible por a y por b, y teniendo en cuenta que (a, b) = 1, es también divisible por ab. Por otra parte, de  $(xu)^{ab} = 1 \pmod{m}$  se deduce (c. § 1) que ab es divisible por  $\delta$ . Por lo tanto,  $\delta = ab$ 

d. Existen raices primitivas respecto del módulo p En efecto, sean

$$\delta_1, \delta_2, \ldots, \delta_r$$
 (1)

todos los exponentes distintos a que pertenecen los números 1. 2. . . (p-1) respecto del módulo p. Supongamos que τ es el mínimo común múltiplo de estos exponentes y que x =  $=q_1^{\alpha_1}, q_2^{\alpha_2} \dots q_k^{\alpha_k}$  es su descomposición canónica. Cada factor que de esta descomposición divide al menos a uno de los números 6, de la sucesión (1), el cual, por consiguiente, puede expresarse en la forma;  $\delta_1 = aq^{\alpha_0}$  Sea  $\xi_i$  uno de los números de la sucesión 1, 2, ..., p-1, pertenecientes al exponente  $\delta_1$ . Según b, el número  $\eta_1 = \xi^{\alpha}$  pertenece al exponente  $q_{a_1}^{\alpha_1}$  y según c, el producto  $g = \eta_1 \eta_1 \dots \eta_k$  pertenece al exponente  $q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k} = \tau$ .

Pero, como todos los números (1) dividen a τ, todos los números 1, 2, ..., p - 1 son soluciones (c, § 1) de la congruencia x a l (mód. p); por esta razón, en virtud de c, § 4, cap. IV, se tiene,  $p-1 \le \tau$  Pero (d, § 1)  $\tau$  es un divisor del número p-1. Por lo tanto,  $\tau = p-1$  y g es una raíz primitiva.

e. Sea g una raiz primitiva respecto del módulo p. Se puede señalar un número t de modo que el número u que se determina por la igualdad  $(g + pl)^{p-1} = 1 + pu$  no sea divisible por p. El número correspondiente g + pt es una raiz primitiva respecto del módulo p $\alpha$  para cualquier  $\alpha > 1$ 

En efecto, se tiene

$$g^{p-1} = 1 + pT_0,$$
  
 $(g + pt)^{p-1} = 1 + p(T_0 - g^{p-1}t + pT) = 1 + pu,$  (2)

donde u, simultaneamente con t, recorre el sistema completo de restos respecto del módulo p. Por lo tanto, se puede indicar un número t de modo que u no sea divisible por p. Para tal valor I, de (2) se deduce también que

$$(g+pt)^{p_1p_2p_3} = (1+pu)^p = 1+p^2u_2, (g+pt)^{p_1p_2p_3} = (1+p^2u_2)^p = 1+p^2u_3,$$

$$(3)$$

donde  $u_2$ ,  $u_3$ , no son divisibles por p

Supongamos que g+pt pertenece al exponente  $\delta$  respecto del módulo  $p^x$  Entonces

$$(g+pt)^b \equiv 1 \text{ (mod. } p^a). \tag{4}$$

De aquí que  $(p+pt)^0 \equiv 1 \pmod{p}$ ; por consiguiente, 0 es un múltiplo de p-1, y como 0 divide a  $\varphi(p^n) = p^{\alpha-1}(p-1)$  se tiene que  $0 = p^{r-1}(p-1)$ , donde r es uno de los números  $1, 2, \ldots, \alpha$ . Sustituyendo el primer miembro de la congruencia (4) por su expresión de la igualdad correspondiente de (2) y (3), resulta  $(u=u_1)$ :

 $1 + p^r u_r = 1 \pmod{p^\alpha}$ ,  $p^r = 0 \pmod{p^\alpha}$ ,  $r = \alpha$ ,  $\delta = \phi(p^\alpha)$ , es decir, g + pi es una raíz primitiva respecto del módulo  $p^\alpha$ .

1. Sea  $g_1$  una ratz primitiva respecto del módulo  $p^{\alpha}$ , donde  $\alpha \ge 1$ . Entonces, el impar entre los números  $g_1$  y  $g_1 + p^{\alpha}$ , es una ratz primitiva respecto del módulo  $2p^{\alpha}$ .

En efecto, es obvio que cualquier número impar x que satisfaga a una de las congruencias  $x^{\gamma} \equiv 1 \pmod{p^{\alpha}}$  y  $x^{\gamma} \equiv 1 \pmod{2p^{\alpha}}$  satisface también a la otra. Por lo tanto, como  $\varphi(p^{\alpha}) = \varphi(2p^{\alpha})$ , cualquier impar x que sea una raíz primitiva respecto de uno de los módulos  $p^{\alpha}$  y  $2p^{\alpha}$  es también una raíz primitiva respecto del otro. Pero, entre las dos raíces primitivas  $g_1$  y  $g_1 + p^{\alpha}$  respecto del módulo  $p^{\alpha}$ , una de ellas es, inevitablemente, impar, por consiguiente, ésta será también una raíz primitiva respecto del módulo  $2p^{\alpha}$ .

**§ 3. Bisqueda** de las raíces primitivas respecto de los módulos  $p^{\alpha}$  y  $2p^{\alpha}$ , donde p es un número primo impar y  $\alpha \geqslant 1$ , pueden buscarse de los módulos aplicando el siguiente teorema general:  $p^{\alpha}$  y  $2p^{\alpha}$  Sea  $c = \varphi(m)$  y sean  $q_1, q_2, \ldots, q_k$  los divisores primos distintos del número c. Para que un número g, que es primo con m, sea una ratz primitiva respecto del módulo m, es necesario y suficiente que este número g no satisfaga a nin-

guna de las congruencias.

$$g^{\frac{c}{q_1}} = 1 \pmod{m}, g^{\frac{c}{q_2}} = 1 \pmod{m}, \dots,$$

$$\cdots g^{\frac{c}{q_k}} = 1 \pmod{m}. \quad (1)$$

En efecto, si g es una raiz primitiva, éste pertenece al exponente c y, por consiguiente, no puede satisfacer a ninguna de las congruencias (1).

Reciprocamente, supongamos que g no satisface a ninguna de las congruencias (1). Si el exponente  $\delta$ , al cual pertenece g, fuese menor que c, entonces, designando con la letra q alguno de los divisores primos de  $\frac{c}{\delta}$ , tendriamos que  $\frac{c}{\delta} = qu$ ,  $\frac{c}{q} \Rightarrow \hbar u$ .  $g^{\frac{c}{q}} = 1$  (mód. p), lo cual contradice a la hipótesia hecha. Por lo tanto,  $\delta = c$  y g es una raiz primitiva. Ejemplo 1. Sea m = 41. Se tiene  $\varphi$  (41) =  $40 = 2^a \cdot 5$ ,  $\frac{40}{5} = 8$ ,  $\frac{40}{2} = 20$ . Por consiguiente, para que un número g, no divisible por 41, sea una raiz primitiva respecto del módu-

$$g^0 = 1 \pmod{41}, g^{00} = 1 \pmod{41}.$$
 (2)

Ensayando los números 2, 3, 4, . . ., hallamos (respecto del módulo 41):

lo 41, es necesario y suficiente que este número g no satisfaga

a ninguna de las congruencias

Vemos, pues, que los números 2, 3, 4, 5 no son raíces primitivas, puesto que cada uno de ellos satisface al menos a una de las congruencias (2). El número 6 es una raíz primitiva, pues no satisface a ninguna de las congruencias (2).

**Ejemplo 2.** Sea  $m=1.681=41^8$  En este caso también se podría buscar una raiz primitiva aplicando el teorema general Sin embargo, la hallaremos más fácilmente aplicando el

teorema e, § 2. Teniendo en cuenta (ejemplo 1) que el número 6 es una raíz primitiva respecto del módulo 41, hallamos:

$$6^{40} = 1 + 41 (3 + 41l),$$

$$(6 + 41l)^{40} = 1 + 41 (3 + 41l - 6^{30}l + 41l) = 1 + 41u.$$

Para que u no sea divisible por 41, es suficiente tomar t=0. Por ello, se puede tomar por raiz primitiva respecto del módulo I 681 el número  $6 + 41 \cdot 0 = 6$ 

Ejemplo 3. Sea m=3 362 = 2·1 681. En este caso también se podría buscar una raíz primitiva aplicando el teorema general. Sin embargo, la hallaremos más fácilmente aplicando el teorema f, § 2. Teniendo en cuenta (ejemplo 2) que el número 6 es una raíz primitiva respecto del módulo 1 681, se puede tomar por raíz primitiva respecto del módulo 3 362 el número impar entre los números 6, 6 + 1 681, o sea, el número 1 687

§ 4. Indices respecto de los módulos pa y 2pa a. Supongamos que p es un número primo impar,  $\alpha \geqslant 1$ ; m es uno de los números  $p^{\alpha}$  y  $2p^{\alpha}$ ,  $c=\phi$  (m), g es una raíz primitiva respecto del módulo m

b. Si  $\gamma$  recorre los restos no negativos mínimos  $\gamma=0,\,1,\,\ldots$ , c — 1 respecto del módulo c, entonces  $g^{\gamma}$  recorre el sistema reducido de restos respecto del módulo m.

En efecto,  $g^n$  recorre c números que son primos con m y que, en virtud de b, § 1, no son congruentes entre si respecto del módulo m.

c. Para los números a que son primos con m introduciremos el concepto de indice, el cual representa una analogía del concepto de logaritmo, en este caso, la raiz primitiva desempeña un pape! similar al de la base de los logaritmos. Si (se supone que  $\gamma \ge 0$ ), el número  $\gamma$  se llama indice del número a, respecto del módulo m, de base g y se designa con la notación  $\gamma = \text{ind } a$  (más exactamente  $\gamma = \text{ing}_g a$ ).

En virtud de b, todo a que sea primo con m admite un índice único y' entre los números de la sucesión

$$\gamma = 0, 1, \ldots, c-1.$$

Una vez conocido  $\gamma'$ , se pueden señalar también todos los indices del número a; según c. § I, éstos serán todos los números no negativos de la clase

De la definición de índice dada se deduce inmediatamente que los números que poseen un índice dado  $\gamma$  forman una clase de números respecto del módulo m.

d. Se tiene

$$\operatorname{ind} ab \ldots l = \operatorname{ind} a + \operatorname{ind} b + \ldots + \operatorname{ind} l \pmod{c}$$

y, en particular,

ind 
$$a^n = n$$
 ind  $a$  (mód.  $c$ ).

En efecto,

$$a = g^{\operatorname{ind} a} \pmod{m}, \quad b = g^{\operatorname{ind} b} \pmod{m}, \dots, \dots, i = g^{\operatorname{ind} l} \pmod{m},$$

de donde, multiplicando, hallamos

$$ab \dots l \equiv g^{\ln d a + \ln d b + \dots + \ln d l}$$
 (mód.  $m$ ).

Por consiguiente, ind  $a + \text{ind } b + \ldots + \text{ind } l$  es uno de los índices del producto  $ab \ldots l$ .

e.. Debido a las aplicaciones prácticas de los índices, para cada módulo p (claro, no muy grande) se han compuesto tablas de indices. Estas son dos: una para hallar el índice de un número dado, otra para hallar los números por el índice. Las tablas contienen los restos no negativos mínimos de los números (el sistema reducido) y sus índices mínimos (el sistema completo) respecto de los módulos p y  $c - \varphi(p) = p - 1$ , respectivamente.

**Ejemplo.** Formemos las tablas indicadas para el módulo p=41. Anteriormente se demostró (ejemplo 1, § 3) que el número g=6 es una raíz primitiva respecto del módulo 41; tomémoslo por base de los índices. Hallamos (las congruencias se toman respecto del módulo 41):

$$6^{9} = 1$$
  $6^{8} = 10$   $6^{16} = 18$   $6^{94} = 16$   $6^{93} = 37$   $6^{1} = 6$   $6^{8} = 19$   $6^{17} = 26$   $6^{29} = 14$   $6^{28} = 17$   $6^{2} = 36$   $6^{10} = 32$   $6^{10} = 33$   $6^{20} = 2$   $6^{34} = 20$   $6^{1} = 11$   $6^{11} = 28$   $6^{10} = 34$   $6^{27} = 12$   $6^{35} = 38$   $6^{4} = 25$   $6^{12} = 4$   $6^{20} = 40$   $6^{31} = 31$   $6^{34} = 23$   $6^{5} = 27$   $6^{15} = 24$   $6^{21} = 35$   $6^{25} = 22$   $6^{37} = 15$   $6^{6} = 39$   $6^{14} = 21$   $6^{22} = 5$   $6^{30} = 9$   $6^{35} = 8$   $6^{7} = 29$   $6^{16} = 3$   $6^{25} = 30$   $6^{31} = 13$   $6^{39} = 7$ 

por lo fanto, las tablas indicadas son:

N	0	1	2	3	4	5	6	7	8	9	1	0	ı	2	3	4	δ	6	7	8	9
	8 34	3 14	27 29	31 36	25 13	37 4	24 17	39 33 5 32	16 11	7	1 2	32 40	28 35	4 5	11 24 30 17	21 16	3 14	18	26 12	33 31	34 22

Aquí el número de la fila denota las decenas y el número de la columna denota las unidades del número (del índice). En la casilla que es común para la fila y columna indicadas viene colocado el índice (el número) correspondiente.

Por ejemplo, el ind 25 se halla en la casilla de la primera tabla que es común a la fila que posee el número 2 y a la columna que posee el número 5, es decir, ind 25 = 4. El número cuyo índice es 33 se halla en la casilla de la segunda tabla que es común a la fila que posee el número 3 y a la columna que posee el número 3, es decir, 33 = ind 17.

- class de la teorla antecedente
- § 5. Consecuen- a. Supongamos que p es un número primo impar; α ≥ 1, m es uno de los números  $p^{\alpha}$ ,  $2p^{\alpha}$ , y, finalmente,  $c = \varphi(m)$ . b. Sea (n, c) = d; entonces
- 1. La congruencia

$$x^n \equiv a \pmod{m}$$
 (1)

admite solución (y, por consiguiente, a es un resto de grado n respecto del módulo m) cuando, y sólo cuando, ind a es un múltiplo de d.

Si la congruencia (1) es resoluble, ésta admite d soluciones.

2. En el sistema reducido de restos respecto del módulo m, el número de restos de grado n es igual  $a = \frac{c}{d}$ .

En efecto, la congruencia (1) es equivalente a la siguiente:

$$n \text{ ind } x = \text{ind } a \text{ (mod. } c),$$
 (2)

la cual admite solución cuando, y sólo cuando, ind a es un múltiplo de d (d, § 2, cap IV).

Si la congruencia (2) admite solución, para el ind x se obtienen d valores incongruentes respecto del módulo c; a éstos les corresponden d valores de x que son incongruentes respecto del módulo et.

Por lo tanto, la afirmación I es cierta.

Entre los números  $0, 1, \dots, c-1$ , los cuales son los indices mínimos de los restos del sistema reducido respecto del módulo  $m_i$  hay  $\frac{c}{d}$  números que son múltiplos de d. Por lo tanto, la afirmación 2 es cierta.

Ejemplo 1. Para la congruencia

$$x^4 = 23 \text{ (mód. 41)}$$
 (3)

se tiene (8, 40) = 8, y como ind 23 = 36 no es divisible por 8, la congruencia (3) es irresoluble.

Elemplo 2. Para la congruencia

$$x^{13} = 37 \text{ (mód. 41)}$$
 (4)

se tiene (12, 40) = 4, y ind 37 = 32 es divisible por 4. Por lo tanto, la congruencia (4) es resoluble y admite 4 soluciones. Las soluciones indicadas se hallan del modo siguiente.

La congruencia (4) es equivalente a las siguientes:

12 ind x = 32 (mód. 40), ind x = 6 (mód. 10).

De aquí, para el ind x se hallan 4 valores incongruentes respecto del módulo 40:

$$ind x = 6, 16, 26, 36,$$

correspondientemente a lo cual se hallan 4 soluciones de la congruencia (4):

$$x = 39$$
; 18; 2; 23 (mód. 41).

Elemplo 3. Los números

cuyos índices son múltiplos de 4, son todos los restos bicuadráticos (o también todos los restos de cualquier grado n = 12, 28, 36, ..., donde (n, 40) = 4), que hay entre los restos positivos mínimos respecto del módulo 41. La cantidad de números en la sucesión (5) es igual a  $10 = \frac{40}{4}$ .

c. Junto con el aserto b. 1 es útil el siguiente:

El número a es un resto de grado n respecto del módulo m cuando, y sólo cuando,

$$a^{\frac{c}{d}} = 1 \text{ (mód. } m). \tag{6}$$

En efecto, la condición ind a=0 (mód. d) es equivalente a la siguiente  $\frac{c}{d}$  ind a=0 (mód. c). Por su parte, esta última es equivalente a la condición (6).

Ejemplo. En el teorema del § 3, la imposibilidad de la congruencia  $g^{\frac{c}{q}} \equiv 1$  (mód. m) es equivalente a la condición de que g sea un no-resto de grado q respecto del módulo m.

En particular, la imposibilidad de la congruencia  $g^{\frac{c}{2}} = 1$  (mód. m) es equivalente a la condición de que g sea un no-resto cuadrático respecto del módulo m (compárese con e, § 1, cap. V).

**6.** 1. El exponente 6, al cual pertenece a respecto del módulo m, se determina por la igualdad (ind. a, c) =  $\frac{c}{b}$ ; en particular, la pertenencia de a al conjunto de raices primitivas respecto del módulo m se determina por la igualdad (ind a, c) = 1.

2. En el sistema reducido de restos respecto del módulo m, la cantidad de números que pertenecen al exponente  $\delta$  es igual  $a \phi(\delta)$ ; en particular, la cantidad de raices primitivas es igual

a \phi (c).

En efecto,  $\hat{\sigma}$  es el divisor mínimo de c que satisface a la condición  $a^{\hat{\sigma}}\equiv 1\pmod{m}$ . Esta condición es equivalente a

 $\delta$  ind a = 0 (mod. c).

o sea,

ind 
$$a = 0 \pmod{\frac{c}{\delta}}$$
.

Por lo tanto,  $\delta$  es el divisor menor de c para el cual  $\frac{c}{\delta}$  divide a ind a, de donde  $\frac{c}{\delta}$  es el divisor mayor de c que divide a ind a, es decir,  $\frac{c}{\delta} = (\text{ind } a, c)$ . Por lo tanto, la afirmación 1 es cierta.

afirmación I es cierta. Entre los números 0, 1, ..., c-1, los cuales son los índices mínimos de los restos del sistema reducido respecto del módulo m, son múltiplos de  $\frac{c}{\delta}$  los números de la forma  $\frac{c}{\delta}y$ , donde  $y=0,1,\ldots,\delta-1$ . La condición  $\left(\frac{c}{\delta}y,c\right)=\frac{c}{\delta}$  equivale a que sea  $(y,\delta)=I$ ; a esta última condición satisfacen  $\varphi(\delta)$  valores de y. Por lo tanto, la afirmación 2 es cierta.

Ejemplo 1. En el sistema reducido de restos respecto del módulo 41, los números que pertenecen al exponente 10 son aquellos números a que satisfacen a la condición (ind a, 40) =

 $=\frac{40}{10}=4$ , es decir, son los números

4, 23, 25, 31,

En total se tienen  $4 = \varphi(10)$  números.

Elempio 2. En el sistema reducido de restos respecto del módulo 41 son raices primitivas los números a que satisfacen a la condición (ind a, 40) = 1, es decir, los números

6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35, En total se tienen  $16 = \phi$  (40) raices primitivas.

- 8 6. Indices a. Para el módulo 2ª la teoría precedente respecto se sustituye por otra un poco más comdel módulo 2ª plicada.
- b. Sea  $\alpha = 1$ . Entonces  $2^{\alpha} = 2$ . Se tiene  $\varphi(2) = 1$ . Es una raiz primitiva respecto del módulo 2, por ejemplo, 1 = = -1 (mod. 2). El número  $1^0 = (-1)^0 = 1$  forma el sistema reducido de restos respecto del módulo 2
- c. Sea  $\alpha = 2$ . Entonces  $2^{\alpha} = 4$ . Se tiene  $\varphi(4) = 2$ . Es una raiz primitíva respecto del módulo 4, por ejemplo, 3 =  $-1 \pmod{4}$  Los números  $(-1)^0 = 1$ ,  $(-1)^1 = 3 \pmod{4}$ forman el sistema reducido de restos respecto del módulo 4.
- d. Sea  $\alpha \geqslant 3$ . Entonces  $2^{\alpha} \geqslant 8$ . Se tiene  $\phi(2^{\alpha}) = 2^{\alpha-1}$ Fácilmente se observa que en este caso no hay raices primitivas: piás exactamente: el exponente al que pertenece un número impar x respecto del módulo 2ª no es superior a

 $2^{\alpha-2} = \frac{1}{2} \varphi(2^{\alpha})$ . En efecto, se tiene

$$x^2 = 1 + 8t_1,$$
  
 $x^4 = 1 + 16t_2,$ 

$$x^{2\alpha-2} = 1 + 2^{\alpha}t_{\alpha-2} = 1 \pmod{2^{\alpha}}$$

Ahora bien, existen números que pertenecen al exponente  $2^{a-2}$ . Tal es, por ejemplo, el número 5. En efecto,

$$5 = 1 + 4,$$

$$5^{2} = 1 + 8 + 16,$$

$$5^{6} = 1 + 16 + 32u_{2},$$

$$5^{2\alpha - 3} = 1 + 2^{\alpha - 1} + 2^{\alpha}u_{\alpha - 2},$$

de donde se ve que ninguna de las potencias  $5^1$ ,  $5^2$ ,  $5^4$ , ...,  $5^{2^{\alpha-3}}$  es congruente con l respecto del módulo  $2^{\alpha}$ . Fácilmente se observa que los números de las dos filas siguientes:

 $5^{0}$ ,  $5^{1}$ , ...,  $5^{2^{\alpha-2}-1}$ ,  $-5^{0}$ ,  $-5^{1}$ , ...,  $-5^{2^{\alpha-2}-1}$ 

forman el sistema reducido de restos respecto del módulo  $2^{\alpha}$  En efecto, en total se tienen  $2\cdot 2^{\alpha-2} = \phi$  ( $2^{\alpha}$ ) números; los números de cada fila por separado son incongruentes entre si respecto del módulo  $2^{\alpha}$  (b, § 1); finalmente, los números de la fila superior son incongruentes con los de la inferior, puesto que, respecto del módulo 4, los primeros son congruentes con 1 mientras que los segundos son congruentes con —1.

e. Para mayor comodidad en las investigaciones posteriores expresaremos los resultados b, c, d en una forma más uniforme, la cual valdrá también para el caso  $\alpha = 0$ .

$$c=1$$
,  $c_0=1$ , so  $\alpha=0$ , o so  $\alpha=1$ ;  
 $c=2$ ,  $c_0=2^{\alpha-2}$ , so  $\alpha\geqslant 2$ ,

(por lo tanto, siempre  $cc_0 = \varphi(2^n)$ ) y supongamos que  $\gamma$  y  $\gamma_0$  recorren, independientemente uno del otro, los restos mínimos no negativos

 $\gamma = 0, \ldots, c-1; \quad \gamma_0 = 0, \ldots, c_0-1$ respecto de los módulos c y  $c_0$ . Entonces  $(-1)^{\gamma}$  5% recorre el sistema reducido de restos respecto del módulo  $2^{\alpha}$ .

### f. La congruencia

$$(-1)^{\gamma} 5^{\gamma_0} \equiv (-1)^{\gamma'} 5^{\gamma'_0} \pmod{2^{\alpha}}$$
 (1)

se verifica cuando, y sólo cuando

$$\gamma = \gamma' \pmod{c}$$
  $\gamma_0 = \gamma'_0 \pmod{c_0}$ .

En efecto, para  $\alpha=0$  el teorema es obvio. Por lo tanto, supongamos que  $\alpha>0$  Sean r y  $r_0$  los restos mínimos no negativos respecto de los módulos c y  $c_0$  para los números  $\gamma$  y  $\gamma_0$ , y sean r' y  $r'_0$  los restos correspondientes para los números  $\gamma'$  y  $\gamma'_0$ . En virtud de c, § 1 (—1 pertenece al exponente c mientras que 5 pertenece al exponente  $c_0$ ), se verifica la congruencia (1) cuando, y sólo cuando, (—1)r' 5r''0 = r''1 (mód 2r''2), es decir, (en virtud de e) cuando r''3 = r''4 g, Si

$$a = (-1)^{\nu} 5^{\nu a} \pmod{2^{\alpha}}$$

el sistema γ, γ<sub>0</sub> se llama sistema de indices del número a respecto del módulo 2<sup>α</sup>

En virtud de e, todo a que sea primo con  $2^{q_i}$  (o sea, impar) admite un sistema único de índices y',  $y'_a$  entre los  $cc_a$ 

φ (2a) pares de valores γ, γο indicados en e

Conociendo el sistema γ', γ', se pueden indicar también todos los sistemas de Indices del número α; según f, éstos serán todos los pares γ, γ<sub>0</sub> formados por las clases de números no negativos

$$y = y' \pmod{c}$$
,  $y_0 = y'_0 \pmod{c_0}$ 

De la definición dada de sistema de índices se deduce inmediatamente que los números que poseen un sistema de índices dado γ. γ<sub>0</sub> forman una clase de números respecto del módulo 2º

h. Los indices del producto son congruentes con las sumas de los indices de los factores respecto de los módulos c y c<sub>0</sub>.

En efecto, sean  $\gamma(a)$ ,  $\gamma_0(a)$ ,  $\gamma(l)$ ,  $\gamma_0(l)$  los sistemas de

Indices de los números  $a, \ldots, l$ . Se tiene

$$a \dots l = (-1)\tau(a)^{\mu} \cdot \tau \tau(b) \cdot 5 \cdot \tau_0(a)^{\mu} \cdot \tau \tau(b)$$

Por consiguiente,  $\gamma(a) + \ldots + \gamma(l)$ ,  $\gamma_0(a) + \ldots + \gamma_0(l)$ son los indices del producto a . . . l.

\$ 7. Indices respecto de cualquier módulo compaesto

b. Si

122

a. Sea  $m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$  la descomposición canónica del número m. Supongamos que c y co denotan los valores indicados en e, 6 6;  $c_s = \phi(p_s^{\alpha_s})$ ;  $g_s$  es la raíz primitiva mínima respecto del módulo pas.

$$a = (-1)^{\gamma} 5^{\gamma_0} \pmod{2^{\alpha_1}},$$

$$a = g_1^{\gamma_1} \pmod{p_1^{\alpha_1}}, \dots, a = g_k^{\gamma_k} \pmod{p_k^{\alpha_k}}.$$
(1)

el sistema y, yo, yı, ..., ya se llama sistema de indices del número a respecto del módulo m.

De esta definición se deduce que y, yo es el sistema de índices del número a respecto del módulo 2ª y y<sub>1</sub>, ..., y<sub>h</sub> son los índices del número a respecto de los módulos  $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ . Por ello (g, § 6; c, § 4), todo a que es primo con m (y que, por consiguiente, es primo con todos los números  $2^a$ ,  $\rho_1^{a_1}$ , ...,  $\rho_k^{a_k}$ ) admite un sistema único de Indices  $\gamma'$ ,  $\gamma_0$ ,  $\gamma_1'$ , ...,  $\gamma_k'$  entre los  $cc_0c_1...c_k = \varphi(m)$  sisternas γ, γ<sub>0</sub>, γ<sub>1</sub>, ..., γ<sub>A</sub> que se obtienen cuando γ, γ<sub>1</sub>, ..., γ<sub>k</sub> recorren, independientemente uno de otro, los restos mínimos no negativos respecto de los módulos c. ca. chi, ..., ch. Formando todos los sistemas y, ye, ye, ..., Ya, compuestos por los números no negativos de las clases

$$\gamma := \gamma_1' \text{ (mód. } c_1), \quad \gamma_0 := \gamma_0' \text{ (mód. } c_0), \\
\gamma_1 := \gamma_1' \text{ (mód. } c_1), \quad \dots, \quad \gamma_k := \gamma_k' \text{ (mód. } c_k).$$

se obtienen todos los sistemas de índices del número a. Los números a que poseen un sistema dado de índices γ, γο.  $\gamma_1, \ldots, \gamma_k$  pueden hallarse resolviendo el sistema (1) y, por consiguiente (b, § 3, cap. IV), forman una clase de números respecto del módulo m.

c. Como los indices  $\gamma_1, \gamma_0, \gamma_1, \ldots, \gamma_k$  del número a respecto del módulo m son los indices del mismo respecto de los módulos  $2^{\alpha}, \rho_1^{\alpha_1}, \ldots, \rho_k^{\alpha_k}$ , respectivamente, subsiste el teorema:

Los indices del producto son congruentes respecto de los módulos  $c, c_0, c_1, \ldots, c_k$  con las sumas de los indices de los factores.

d. Sea  $\tau = \varphi(2^{\alpha})$  si  $\alpha \leqslant 2$  y  $\tau = \frac{1}{2} \varphi(2^{\alpha})$  si  $\alpha > 2$  y designemos con h el mínimo común múltiplo de los números  $\tau$ ,  $c_1, \ldots, c_k$ . Para cualquier  $\alpha$  que sea primo con m, se cumple la congruencia  $a^h = 1$  respecto de todos los módulos  $2^{\alpha}$ ,  $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ , por lo cual, también se cumple esta congruencia respecto del módulo m. Por lo tanto, a no puede ser una raíz primitiva respecto del módulo m si  $h < \varphi(m)$ . Pero esto último ocurre cuando  $\alpha > 2$  siendo k > 1, y también cuando  $\alpha = 2$ , k = 1. Por consiguiente, para m > 1 pueden existir raíces primitivas solamente en los casos m = 2, 4,  $p_1^{\alpha_1}$ ,  $2p_1^{\alpha_1}$ . Pero precisamente en estos casos fue demostrada anteriormente (§ 6, § 2) la existencia de raíces primitivas. En resumen, todos los casos en que existen raíces primitivas respecto de un módulo m, superior  $\alpha$  1, son

 $m=2, 4, p^{\alpha}, 2p^{\alpha}$ 

## Pregantas referentes al capitulo VI

A continuación, la letra p siempre denota un número primo impar, y en la pregunta 11, b, también el número 2.

1, a. Sea a un número entero, a > 1. Demostrar que los divisores primos impares del número  $a^p - 1$  dividen a a - 1 o son de la forma 2px + 1.

- b. Sea a un número entero, a > 1. Demostrar que los divisores primos impares del número  $a^p + 1$  dividen a a + 1 o son de la forma 2ax + 1.
- c. Demostrar que hay una cantidad infinita de números primos de la forma 2px + 1.
- d. Sea n un número entero, n > 0 Demostrar que los divisores primos del número  $2^{n} + 1$  son de la forma  $2^{n+1}x + 1$ .
- 2. Sea a un número entero, a > 1, y sea n un número entero, n > 0. Demostrar que  $\varphi(a^n 1)$  es un múltiplo de n.
- 3, a. Sea n un número entero, n > 1. Con los números 1,
- $2, \ldots, n$ , siendo n impar, formemos las permutaciones

1, 3, 5, ..., 
$$n = 2$$
,  $n$ ,  $n = 1$ ,  $n = 3$ , ..., 4, 2, 1, 5, 9, ..., 7, 3,

etc. y siendo n par, formemos las permutaciones

1, 3, 5, ..., 
$$n-1$$
,  $n$ ,  $n-2$ , ..., 4, 2, 1, 5, 9, ..., 7, 3,

etc. Demostrar que la k-ésima operación da la sucesión inicial cuando, y sólo cuando,  $2^h \equiv \pm 1 \pmod{2n-1}$ 

b. Sean n y m dos números enteros, n > 1, m > 1. Contemos los números 1, 2, ..., n en orden directo desde 1 hasta n, después en orden inverso desde n hasta 2, fuego de nuevo en orden directo desde 1 hasta n, después otra vez en orden inverso desde n hasta 2, etc. En este cálculo, escribamos los números: el 1°, el (m+1)-ésimo, el (2m+1)-ésimo, etc., hasta que se obtengan n números. Repitamos la misma operación con la nueva sucesión de n números, etc. Demostrar que la k-ésima operación de la sucesión inicial cuando, y sólo cuando,

 $m^k = \pm 1 \pmod{2n-1}$ .

Demostrar la existencia de φ (δ) números pertenecientes al exponente δ, considerando para ello la congruencia x<sup>6</sup> ≈ π (mód. p) (pregunta 10, c, cap. IV) y aplicando d, § 3, cap. II.

- 5, a. Demostrar que el número 3 es una raiz primitiva de los números primos de la forma  $2^n + 1$ , n > 1.
- b. Demostrar que el número 26-2 es una raiz primitiva de los números primos de la forma 2p+1, según que el número p sea de la forma 4n+1 o de la forma 4n+3.
- c. Demostrar que el número 2 es una raiz primitiva de los números primos de la forma 4p + 1.
- d. Demostrar que el número 3 es una raiz primitiva de los números primos de la forma

$$2^n p + 1$$
, so  $n > 1$  y  $p > \frac{3^{2^{n-1}}}{2^n}$ .

**6, a.**  $\alpha$ ) Sea n entero,  $n \ge 0$ ,  $S_n = 1^n + 2^n + \ldots + (p-1)^n$ . Demostrar que

 $S_n = -1 \pmod{p}$ , si *n* es un múltiplo de p-1,  $S_n = 0 \pmod{p}$  en caso contrario.

β) Conservando las notaciones de la pregunta 9, c, cap. V, demostrar que

$$S(1) = -\left(\frac{\rho-1}{2} \atop \frac{\rho-1}{1}\right) \pmod{\rho}.$$

- b. Demostrar el teorema de Wilson aplicando b, § 4.
- 7. Supongamos que g y  $g_1$  son raíces primitivas respecto del módulo p, y que  $\alpha$  ind  $g_1 = 1 \pmod{p-1}$ .
- a. Sea (a, p) 1 Demostrar que

$$\operatorname{ind}_{d_1} a = a \operatorname{ind}_{d} a \pmod{p-1}$$
.

- b. Sea n un divisor de p-1, 1 < n < p-1. Los números que son primos con p pueden dividirse en n clases, refiriendo a la s-ésima clase  $(s-0,1,\ldots,n-1)$  los números que satisfacen a la condición ind a=s (mód n). Demostrar que la clase de orden s según la base g es equivalente a la clase de orden  $s_1$  según la base  $g_1$ , donde  $g_1 \equiv a$   $g_2 \in a$
- 8. Señalar el método más simple posible de resolución de la congruencia  $x^n = a \pmod{p}$  (que sea cómodo si (n, p 1) no

es muy grande) en el caso en que se conoce una raíz primitiva g respecto del módulo p.

**9.** Supongamos que m, a, c,  $c_0$ ,  $c_1$ , ...,  $c_h$ ,  $\gamma$ ,  $\gamma_0$ ,  $\gamma_2$ , ...,  $\gamma_h$  denotan los valores indicados en el § 7. Tomando cualesquiera raíces R,  $R_0$ ,  $R_1$ , ...,  $R_h$  de las ecuaciones

$$R^{e}=1, \quad R_{4}^{e_{0}}=1, \quad R_{1}^{e_{1}}=1, \ \ldots, \ R_{h}^{e_{h}}=1.$$

hacemos

$$\chi(a) = R^{\gamma} R_{\bullet}^{\gamma_0} R_1^{\gamma_1}, \ldots, R_{\bullet}^{\gamma_h}.$$

Si (a, m) > 1, hacemos  $\chi(a) = 0$ .

La función definida de este modo para todos los valores enteros de  $a_i$  la llamaremos carácter respecto del módulo m. Si  $R = R_0 = R_1 = \ldots, = R_k = 1$ , al carácter lo llamaremos principal; éste admite el valor 1 si (a, m) = 1 y el valor 0 si (a, m) > 1.

- a. Demostrar que del modo indicado se obtienen  $\varphi$  (m) caracteres distintos (dos caracteres se llaman distintos, si al menos para un valor de a éstos no son iguales entre si).
- b. Deducir las propiedades siguientes de los caracteres:
- $\alpha$ )  $\chi(1) = 1$ ,
- $\beta) \ \ \chi(a_1a_2) = \chi(a_1) \chi(a_2),$
- y)  $\chi(a_1) = \chi(a_2)$ , si  $a_1 = a_1 \pmod{m}$ .
- c. Demostrar que

$$\sum_{\alpha=0}^{m-1} \chi(\alpha) = \begin{cases} \varphi(m) & \text{para el carácter principal,} \\ 0 & \text{para los demás caracteres.} \end{cases}$$

d. Demostrar que, sumando para un valor de a dado respecto de todos los  $\varphi(m)$  caracteres, se tiene

$$\sum_{a} \chi(a) = \begin{cases} \varphi(m), & \text{si } a = 1 \text{ (mod. } m), \\ 0 & \text{en caso contrario.} \end{cases}$$

e. Considerando la suma

$$H = \sum_{\mathbf{y}} \sum_{a} \frac{\chi(a)}{\Psi(a)}$$

donde a recorre el sistema reducido de restos respecto del módulo m, demostrar que la función  $\psi$  (a), definida para todos los valores enteros de a y que satisface a las condiciones:

$$\psi(a) = 0$$
, si  $(a_1 \ m) > 1$ ,  
 $\psi(a)$  no es idénticamente igual a 0,  
 $\psi(a_1 a_2) = \psi(a_1) \psi(a_2)$ ,  
 $\psi(a_1) = \psi(a_2)$ , si  $a_1 = a_2 \pmod{m}$ ,

es un carácter.

t. Demostrar los teoremas siguientes.

α) S<sub>1</sub>  $\chi_1(a)$  y  $\chi_2(a)$  son dos caracteres, entonces  $\chi_1(a)$   $\chi_2(a)$  también es un carácter.

β) Si  $\chi_i(a)$  es un carácter y  $\chi(a)$  recorre todos los caracteres, entonces  $\chi_i(a) \chi(a)$  también recorre todos los caracteres.

y) Si (l, m) = 1, se tiene

$$\sum_{x} \frac{\chi(a)}{\chi(l)} = \begin{cases} \varphi(m), & \text{si } a = 1 \pmod{m} \\ 0 & \text{en caso contrario.} \end{cases}$$

10, a. Sea n divisor de p-1, 1 < n < p-1, y l un entero que no sea divisible por n. El número  $R_1 = e^{2\pi i \frac{1}{n}}$  es una raiz de la ecuación  $R_1^n = 1$  y, por consiguiente, la potencia  $e^{2\pi i \frac{l \ln d x}{n}}$ , a la cual hay que asignarle el valor 0 cuando x es un múltiplo de p, es un carácter respecto del módulo p.  $\alpha$ ) Demostrar que si  $(k, p) \sim 1$ , se tiene

$$\sum_{n=1}^{p-1} e^{2\pi i \frac{i \ln d (x+h) - i \ln d x}{n}} = -1$$

β) Sea Q entero.  $1 < Q < \rho$ ,

$$S = \sum_{n=0}^{p-1} |S_{I_n \cdot n, \cdot n}|^2; \quad S_{I_n \cdot n, \cdot n} = \sum_{n=0}^{Q-1} e^{\frac{2\pi i}{n}} \frac{i \operatorname{ind} (n+s)}{n}$$

Demostrar que S = (p - Q)Q.

11, a. Supongamos que a es un entero, n es divisor de p-1,  $1 < n \le p-1$ , k es un entero que no es divisible por n,

$$U_{a,p} = \sum_{n=1}^{p-1} e^{2\pi i \frac{h \ln dx}{n}} e^{2\pi i \frac{ax}{p}}$$

a) Siendo (a, p) = 1, demostrar que  $|U_{a,p}| = \sqrt{p}$ 

β) Demostrar que

$$e^{2\pi i \frac{-\lambda \log a}{n}} = \frac{U_{a,p}}{U_{i,-}}.$$

y) Supongamos que p es de la forma 4m + 1.

$$S = \sum_{k=1}^{p-2} e^{2\pi i \frac{\ln d (x^2 + \pi)}{4}}$$

Demostrar que  $p = A^2 - B^2$  (compárese con las preguntas 9, a y 9, c, cap. V), donde A y B son enteros, definidos por la igualdad S = A + Bt

ô) Supongamos que  $x_a$  recorre los números del sistema reducido de restos respecto del módulo p que satisfacen a la condición ind  $x_a = s \pmod{n}$ . Haciendo

$$S = \sum_{x_1} e^{2\pi i \frac{\alpha x_0}{p}},$$

demostrar que

$$\left|S + \frac{1}{n}\right| < \left(1 - \frac{1}{n}\right) \sqrt{p}.$$

**b.** Sea *n* entero, n > 2, m > 1, (a, m) - 1,

$$S_{a,\,m} = \sum_x e^{2\pi i\,\frac{\alpha x^n}{m}}, \quad S_{a\,\,m}' = \sum_{\underline{x}}' e^{2\pi i\,\frac{\alpha \xi^n}{m}},$$

donde x recorre el sistema completo y  $\xi$  el sistema reducido de restos respecto del modulo m (compárese con la pregunta 12, d, cap. III y con la pregunta 11, b, cap. V)

α) Sea  $\delta = (n, p-1)$ . Demostrar que  $|S_{a,p}| \le (\delta-1)\sqrt{p}$ .

β) Sea 
$$(n, p) = 1$$
 y sea s un entero,  $1 < s < n$ . Demostrar que  $S_{a, p^1} = p^{a-1}, S'_{a, p^1} = 0$ .

γ) Sea s un entero, s > n. Demostrar que

$$S_{a_{1}p^{0}} = p^{n-1}S_{a_{1}p^{n-n}}, S'_{a_{1}p^{0}} = 0.$$

d) Demostrar que

$$|S_{a,m}| < Cm^{1-\frac{1}{n}}$$

donde C depende solamente de n.

12. Sean M y Q enteros,  $0 \le M < M + Q \le p$ .

a. Supongamos que n es un divisor de p-1, 1 < n < < p-1, k es un entero, no divisible por n. Demostrar que

$$\big|\sum_{z=M}^{M+Q-1}e^{2\pi i\frac{h\ln dx}{n}}\big|<\sqrt{\rho}\ln\rho.$$

b,  $\alpha$ ) Sea T la cantidad de números de la s-ésima clase de la pregunta 7, b, comprendidos entre los números M,  $M+1, \ldots, M+Q-1$ . Demostrar que

$$T = \frac{Q}{n} + \theta \sqrt[n]{p} \ln p; \quad \theta_1 < 1.$$

β) Sea N un entero arbitrario y  $l_0 = [2n \sqrt[3]{p} - 1]$  Demostrar que entre los números de la s-ésima clase de la pregunta 7, b existe al menos uno que es congruente respecto del módulo p con alguno de los números de la sucesión

$$N = t_0, \dots, N = 1, N, N + 1, \dots, N + t_0$$

c. Supongamos que k denota el número de divisores primos de p-1 y que M es el número de raíces primitivas respecto del módulo p, comprendidas entre los números M, M+1, . . . , M+Q-1. Demostrar que

$$H = \frac{\varphi(p-1)}{p-1} Q + \theta 2^k \sqrt{p} \ln p, \quad |\theta| < 1.$$

d. Supongamos que  $M_1$  y  $Q_1$  son enteros,  $0 \le M_1 < M_1 + Q_1 \le p-1$ , y que J denota la cantidad de números de la sucesión ind M, and  $(M+1), \ldots$ , ind (M+Q-1), comprendidos entre los números de la sucesión  $M_1$ ,  $M_1 + 1$ ,  $\ldots$ ,  $M_1 + Q_1 - 1$ . Demostrar que

$$J = \frac{QQ_1}{p-1} + \theta \sqrt{p} (\ln p)^2; \quad |\theta| < 1.$$

13. Demostrar la existencia de una constante  $p_0$  que satisface a la condición: si  $p > p_0$ , n es un divisor de p-1, 1 < n < p-1, entonces, el menor entre los no-restos positivos de grado n respecto del módulo p, es < h;

$$h = \rho^{\frac{1}{\alpha}} (\ln \rho)^2; \ c = 2e^{1-\frac{1}{n}}.$$

14, a. Sea m > 1, (a, m) = 1,

$$S = \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} v(x) \rho(y) e^{2\pi i \frac{\alpha x y}{m}},$$

$$\sum_{x=0}^{m-1} |v(x)|^2 + X, \quad \sum_{y=0}^{m-1} |\rho(y)|^2 = Y.$$

Demostrar que  $|S| \leq V \overline{XYm}$ .

b,  $\alpha$ ) Supongamos que m > 1, (a, m) = 1, n es un entero, n > 0, K es el número de soluciones de la congruencia  $x^n = 1 \pmod{m}$ ,

$$S = \sum_{i=1}^{m-1} \chi(x) e^{2\pi i \frac{-nx^n}{m}}.$$

Demostrar que  $|S| \leq K \sqrt{m}$ .

β) Sea a una constante positiva arbitraria. Siendo n constante, demostrar para el número K de la pregunta  $\alpha$ ) que  $K = O(m^2)$ .

c. Sean 2,  $q_2, \ldots, q_k$  los divisores primos distintos del número p-1.

 $\alpha$ ) Supongamos que g recorre las raíces primitivas respecto del módulo p, comprendidas en el sistema reducido de

restos, (a, p) = 1,

$$S = \sum_{p} e^{2\pi i \frac{a_{p}}{p}}.$$

Demostrar que

$$|S| < \frac{9}{8} \frac{\varphi(p-1)}{p-1} 2^k \sqrt{p}$$
.

Para la demostración se debe hacer recorrer a s y s' los números que satisfacen a las condiciones respectivas:

$$0 \leqslant s < p-1; \ s = 0 \ (\text{mod. 2});$$

$$s = s_r \ (\text{mod. } q_r), \quad 0 \leqslant s_r \leqslant \frac{q_r-1}{2} \quad (r=2, \ldots, k),$$

$$0 \leqslant s' < p-1; \quad s' = 1 \ (\text{mod. 2});$$

$$s' = s'_r \ (\text{mod. } q_r), \quad 0 \leqslant s'_r \leqslant \frac{q_r-1}{2} \quad (r=2, \ldots, k),$$

y se debe considerar la suma

$$W = \sum_{i} S_{i}; \quad S_{i} = \sum_{i} \sum_{i'} e^{2\pi i \frac{\alpha u_{i} v_{i}}{p}}, \quad u_{i} = g_{0}^{t_{i}}, \quad v_{i} = g_{0}^{t_{0}},$$

donde t recorre el sistema reducido de restos respecto del módulo p y  $g_0$  es una de las raíces primitivas.

β) Sean M y Q enteros,  $0 \le M \le M + Q \le p$ . Demostrar que la cantidad T de raíces primitivas respecto del módulo p, contenidas en la serie M, M+1, ..., M+Q-1, se expresa por la fórmula

$$T = \frac{\phi\left(\rho - 1\right)}{\rho - 1} \left( Q + \theta \cdot \frac{9}{8} \cdot 2^h \sqrt[p]{\rho} \ln \rho \right) \; ; \quad |\theta| < 1 \, .$$

γ) Sea N un número entero y  $l_0 = \left[\frac{l_2}{6} 2^h \sqrt{\rho}\right]$ . Demostrar que existe una raíz primitiva respecto del módulo  $\rho$  que es congruente con alguno de los números

$$N-l_0, \ldots, N-l_1, N, N+l_1, \ldots, N+l_0.$$

15, a. Supongamos que (a, p) = (b, p) 1, y sea n un número entero distinto de 1,  $|n| = n_1$ ,  $0 < n_1 < p$ ,

$$S = \sum_{x=1}^{p-1} e^{2\pi i \frac{ax^n + bx}{p}}.$$

Demostrar que

$$|S| < \frac{3}{9} n_1^{\frac{1}{2}} p^{\frac{3}{6}}$$

b. Sea (A, p) = 1 y supongamos que n es un entero, distinto de 1,  $|n| = n_1$ ,  $0 < n_1 < p$ ,  $M_0$  y  $Q_0$  son enteros,  $0 < M_0 < M_0 + Q_0 < p$ .

$$S = \sum_{n=M_0}^{M_0+Q_0-1} e^{\frac{2\pi i}{n} \frac{Ax^n}{p}}.$$

Demostrar que

$$|S| < \frac{3}{2} n_1^{\frac{1}{2}} \rho^{\frac{3}{4}} \ln \rho$$
.

β) Supongamos que M y Q son enteros,  $0 \le M < M + Q \le p$ , T es la cantidad de números de la sucesión  $Ax^n$ ,  $x = M_0$ ,  $M_0 + 1, \ldots, M_0 + Q_0 - 1$ , que son congruentes respecto del módulo p con los números de la sucesión M, M + 1, ... M + Q - 1.

Demostrar que

$$T = \frac{Q_0 Q}{\rho} + \theta \frac{3}{2} \pi_1^{\frac{1}{2}} \rho^{\frac{3}{4}} (\ln \rho)^3; \quad |\theta| < 1.$$

c. Supongamos que (a, p) = 1 y sean b y c enteros,  $(b^a - 4ac, p) = 1$ .

a) See y un entero,

$$S = \sum_{n=0}^{p-1} \left( \frac{ax^2 + bx + c}{\rho} \right) e^{2\pi i \frac{\sqrt{x}}{\rho}}.$$

Demostrar que  $|S| < \frac{3}{2} p^{\frac{3}{4}}$ .

 $\beta$ ) Sean M y Q enteros,  $Q \leqslant M \leqslant M + Q \leqslant p$ ,

$$S = \sum_{x=M}^{M+Q-1} \left( \frac{ax^{0}+bx+c}{p} \right).$$

Demostrar que  $|S| < \frac{3}{2} p^{\frac{3}{4}} \ln p$ .

### Ejercicios numéricos referentes al capitalo VI

- 1, a. Hallar (mediante los cálculos más simples posible) el exponente
- al cual pertenece el número 7 respecto del módulo 43
- b. Hallar el exponente al cual pertenece el número 5 respecto del módulo 108.
- 2. a. Hallar las raices primitivas respecto de los módulos 17, 289, 578
- Hallar las raices primitivas respecto de los módulos 23, 529, 1 058.
- c. Hallar la raíz primitiva minima respecto del módulo 242.
- 3, a. Formar la tabla de Indices respecto del módulo 17.
- b. Formar la tabla de indices respecto del módulo 23.
- 4, a. Hallar una raiz primitiva respecto del módulo 71, empleando la nota del elemplo c. 6 5.
- b. Haller una raiz primitiva respecto del módulo 191.
- 8, a. Sirvièndose de la tabla de indices, indicar la cantidad de soluciones de las congruencias:
- $\alpha$ ),  $x^{40} = 79 \pmod{97}$ ,  $\beta$ )  $x^{44} = 17 \pmod{97}$ ,  $\gamma$ )  $x^{16} = 48 \pmod{97}$
- b. Indicar la cantidad de soluciones de las congruencias.
- a)  $3x^{19} = 31 \pmod{41}$ , b)  $7x^7 = 11 \pmod{41}$ , y)  $5x^{19} = 37 \pmod{41}$ .
- 6, a. Sirvièndose de la tabla de indices, resolver las congruencias

$$\alpha$$
)  $x^{0} = 59 \pmod{67}$ ,  $\beta$ )  $x^{00} = 17 \pmod{67}$ ,  $\gamma$ )  $x^{00} = 14 \pmod{67}$ 

b. Resolver les congruencies:

(a) 
$$23x^4 = 15 \pmod{73}$$
,  $\beta$ )  $37x^5 = 69 \pmod{73}$ , y)  $44x^{61} = 53 \pmod{73}$ 

7, a. Aplicando el teorema c. § 5, determinar la cantidad de soluciones de las congruencias

$$\alpha$$
)  $x^0 = 2 \pmod{37}$ ,  $\beta$ )  $x^{16} = 10 \pmod{37}$ 

b. Determinar la cantidad de soluciones de las congruencias:

α) 
$$x^0 = 3 \pmod{.71}$$
, β)  $x^{01} = 5 \pmod{.71}$ .

- 8, a. Empleando el método de la pregunta 8, resolver las congruencias (al resolver la segunda congruencia se debe utilizar la tabla de rafces primitivas que viene inseriada al final del libro):
  - $\alpha$ )  $x^2 = 37 \pmod{101}$ ,  $\beta$ )  $x^4 = 44 \pmod{101}$ .
- b. Resolver la congruencia

- e. Empleando la tabla de indices, indicar, entre los restos del sistema reducido de restos respecto del módulo 19: α) los restos cuadráticos. B) los restos cúbicos.
- Indicar, entre los restos del sistema reducido de restos respecto del módulo 37: α) los restos de grado 15, β) los restos de grado 8.
- 10, a. Indicar, entre los restos del sistema reducido de restos respecto del módulo 43:  $\alpha$ ) los números que pertenecen al exponente 6,  $\beta$ ) las raices primitivas.
- b. Indicar entre los restos del sistema reducido de restos respecto del módulo 61:  $\alpha$ ) los números que pertenecen al exponente 10,  $\beta$ ) las raíces primitivas.

## Respuestas a las preguntas

Respuestas a las preguntas del capitulo !

1. El resto de la division de ax + by por d, teniendo la forma ax' + by' y siendo menor que d, es necesariamente igual a cero. Por elto, d es un divisor de todos los números de la forma ax + by y, en particular, es un divisor comun de los números  $a \cdot 1 + b \cdot 0 = a$  y  $a \cdot 0 + b \cdot 1 = b$ . Por otra parte, la expresión de d muestra que todo divisor común de los números  $a \cdot y \cdot b$  divide  $a \cdot d$ . Por lo tanto, d = (a, b) y el teorema 1, d,  $\frac{1}{2}$  2 es justo. Los teoremas e,  $\frac{1}{2}$  2 se demuestran as: el menor número positivo de la forma  $\frac{a}{3}x + \frac{b}{3}y$  es  $\frac{a}{3}x_0 + \frac{b}{3}y_0$ ; el menor número positivo de la forma  $\frac{a}{3}x + \frac{b}{3}y$  es  $\frac{a}{3}x_0 + \frac{b}{3}y_0$ 

La generalización de estos resultados es trivial

2. Sea  $\delta' = \frac{k}{4}$  una fracción irreducible con la condición  $0 < 1 < Q_s$ . Para  $\delta_s = \alpha$  el teorema es evidente. Por ello, suponemos que  $\delta_s$  no es gual a  $\alpha$  y que, por consiguiente, existe  $\delta_{s+1}$  Limitémonos al caso  $\delta_s < \delta_{s+1}$ . Está claro que

$$|\delta'-\delta_s|<\frac{1}{IQ_s}>\frac{1}{Q_{s+1}Q_s}, \quad |\delta'-\delta_{s+1}|>\frac{1}{IQ_{s+1}}>\frac{1}{Q_{s+1}Q_s}.$$

Por esto, no puede ser  $\delta_a \leqslant \delta' \leqslant \delta_{a+1}$  y, por lo tanto, o  $\delta' < \delta_a$ , o bien  $\delta_{a+1} < \delta'$ . En ambos casos  $\delta_a$  está más proximo a  $\alpha$  que  $\delta'$ . 3. Si  $n \leqslant \delta$  el teorema es evidente; por lo tanto, suponemos que  $n > \delta$  Se tiene

$$\xi = \frac{1 + \sqrt{5}}{2} = 1,618 \quad \text{log}_{10} \ \xi = 0, 2 \quad \text{.}$$

$$Q_2 \geqslant 1 \qquad = g_1 = 1,$$

$$Q_3 \geqslant Q_3 + 1 \qquad \geqslant g_3 = 2 \geqslant \xi,$$

$$Q_4 \geqslant Q_3 + Q_2 \qquad \geqslant g_3 + g_2 + g_1 \geqslant \xi + 1 = \xi^2,$$

$$Q_n \geqslant Q_{n-1} + Q_{n-2} \geqslant g_{n-1} = g_{n-2} + g_{n-3} \geqslant \xi^{n-3} + \xi^{n-4} = \xi^{n-3}.$$

De aqui que

$$N > \xi^{m-1}$$
,  $n < \frac{\log_{10} N}{\log_{10} \xi} + 2 < 5k + 2$ ;  $n < 5k + 1$ .

4, a. Para las fracciones  $\frac{0}{1}$  y  $\frac{1}{1}$  se tiene  $0 \cdot 1$   $1 \cdot 1 = -1$ . Intercalando la fracción  $\frac{A+C}{B+D}$  entre las fracciones  $\frac{A}{B}$  y  $\frac{C}{D}$  que satisfacen a la condición AD-BC=-1, se tiene  $A\left(B+D\right)-B\left(A+C\right)=\left(A+C\right)D$   $-\left(B+D\right)C=-1$ . Por lo tanto, es cierta la atirmación señalada al linal de la pregunta. La existencia de una fracción  $\frac{k}{l}$  con las condicion

nes  $\frac{a}{b}<\frac{k}{l}<\frac{c}{d}$  ,  $l\leqslant \tau$ , es imposible. En caso contrario se fendi la que

$$\frac{k}{l} - \frac{a}{b} > \frac{1}{lb} \; ; \; \frac{c}{d} - \frac{k}{l} > \frac{1}{ld} \; ; \; \frac{a}{d} - \frac{a}{b} > \frac{b+d}{lbd} > \frac{1}{bd} \; .$$

b. Está claro que es suficiente considerar el caso  $0 \leqslant a \leqslant 1$ . Supongamos que  $\frac{a}{b} \leqslant a \leqslant \frac{c}{d}$ , donde  $\frac{a}{b}$  y  $\frac{c}{d}$  son fracciones consecutivas de la sucesión de Farey, correspondientes a  $\tau$ . Son posibles dos casos:

$$\frac{a}{b} < \alpha < \frac{a+c}{b+d}$$
;  $\frac{a+c}{b+d} < \alpha < \frac{c}{d}$ .

Por lo tanto, se verifica una de las dos desigualdades

$$\left|a-\frac{a}{b}\right|<\frac{1}{b(b+d)};\quad \left|d-\frac{c}{d}\right|<\frac{1}{d(b+d)},$$

de donde, en virtud de que  $b+d>\tau$ , se deduce inmediatamente el teorema indicado.

e. Si  $\alpha$  es una fracción irreducible  $\alpha = \frac{a}{b}$  con la condición  $b \leqslant \tau$ .

por  $\frac{P}{Q}$  se puede tomar la fracción misma  $\frac{a}{b}$ . En caso contrario, por  $\frac{P}{Q}$  se puede tomar la fracción roducida  $\frac{P_g}{Q_g}$  que cumple la condición  $Q_g \ll \pi \ll Q_{g+1}$ .

5, a. Los residuos que resultan al dividir los números primos impares por 4 son iguales a 1 ó a 3. El producto de números de la forma 4m+1 es de la forma 4m+1. Por lo tanto, el número  $4p_1 \ldots p_k-1$ , donde  $p_1, \ldots, p_k$  aon primos de la forma 4m+3, tiene que tener un divisor primo q de la forma 4m+3. El número q no coincide con nínguno de los números  $p_1, \ldots, p_k$ .

b. Los números primos superiores a 3 son de la forma 6m+1 o de la forma 6m+5. El número  $6p_1$  ,  $p_h-1$ , donde  $p_1$ , . .,  $p_h$  son primos de la forma 6m+5, tiene que tener un divisor primo q de la forma 6m+5. El número q no coincide con ninguno de los números  $p_1, \ldots, p_h$ .

6. Supongamos que  $p_1, \ldots, p_k$  son k números primos cualesquiera y sea N un entero que cumpia las condiciones 2 < N,  $(3 \text{ in } N)^k < N$ . La cantidad de números a de la sucesión  $1, 2, \ldots, N$ , cuyas descomposiciones canónicas tienen la forma  $a = p_1^{a_1} \ldots p_k^{a_k}$  no es superior a

$$\left(\frac{\ln N}{\ln 2} + 1\right)^h < (3 \ln N)^h < N,$$

puesto que  $\alpha_0 < \frac{\ln N}{\ln 2}$ .

Por lo tanto, en la sucesión 1, 2, ..., N hay números en cuyas descomposiciones canónicas figuran primos distintos de  $p_1$ , ...,  $p_k$ . 7. Se obtienen tales sucesiones, por ejembo, para

$$M = 2 \cdot 3 \ldots (K + 1) t + 2; t = 1, 2, \ldots$$

**6.** Tomando un entero  $z_0$  con la condición de que para  $x \gg z_0$  sea f(x) > 1 y f'(x) > 0, hagamos  $f(x_0) = X$ . Todos ios números  $f(x_0 + Xt)$ , t = 1, 2, son compuestos (múltiplos de X)

 $\Theta$ , a. Si se cumple (1), entonces uno de los números x, y es par, sea x par De la igualdad

$$\left(\frac{x}{2}\right)^2 = \frac{z+y}{2} \cdot \frac{z-y}{2} \,,$$

donde, evidentemente,  $\left(\frac{x+y}{2}, \frac{x-y}{2}\right) = 1$ , nos convencemos de la existencia de números enteros positivos u y v que cumplen las condiciones

$$\frac{x}{2} = uv, \qquad \frac{z+y}{2} = u^2, \qquad \frac{z-y}{2} = v^2.$$

De aqui se deduce que las condiciones indicadas en la pregunta son necesarias

Es obvio que dichas condiciones son suficientes.

b. Convengemos en designar aqui con letras solamente los números enteros positivos. Supongamos que existen sistemas x, y, z, que cumplen las condiciones  $x^4 + y^4 = z^3$ , x > 0, y > 0, z > 0, (x, y, z) = 1; elijamos entre ellos el sistema con el valor menor de z Suponiendo que x es par, obtenemos  $x^4 = 2uv$ ,  $y^3 = u^3 - v^2$ , u > v > 1, (u, v) = 1, donde v es par (si u fuese par, tendriamos  $y^4 = 4N + 1$ ,  $u^3 = 4N_1$ ,  $v^4 = 4N_3 + 1$ ,  $4N + 1 = 4N_3 - 4N_3 - 1$ , lo cual es

imposible). De aquí que

$$u = z_1^2$$
,  $v = 2w^2$ ,  $y^2 + 4w^4 = z_1^4$ ,  $2w^2 = 2u_1v_1$ ,

 $u_1 = x_1^a$ ,  $v_1 = y_1^a$ ,  $x_1^a + y_1^a = x_1^a$ , lo cual es imposible, puesto que  $z_1 < z$ . De la irresolubilidad de la ecuación  $x^4 + y^4 = z^a$ , como un caso particular se deduce también, evidentemente, la irresolubilidad de la ecuación  $x^4 + y^4 = t^4$  en enteros positivos x, y, t.

10. Haciendo  $x = \frac{k}{l}$ ; (k, l) = 1, obtenemos

$$k^n + a_1 k^{n-1} l + \ldots + a_n l^n = 0.$$

Por lo tanto,  $k^n$  es un múltiplo de l y, por consiguiente, l=1.

If, a. Supongamos que k es el mayor número entero que cumple la condición  $2^k \le n$  y sea P el producto de todos los números impares que no son superiores a n. El número  $2^{k-1}PS$  se expresa en forma de una suma cuyos términos, a excepción de  $2^{k-1}P\frac{1}{2^k}$ , son números

enteros

b. Supongamos que k es el mayor número entero que cumple la condición  $3^k < 2n+1$  y sea P el producto de todos los números que son primos con el número 6 y que no son superiores a 2n+1 El número  $3^{k-1}PS$  se expresa en forma de una suma cuyos términos, a excepción de  $3^{k-1}P$  son números enteros

12. Para n < 8 el teorema se comprueba inmedialamente. Por lo tanto, suponiendo que n > 8 y que el teorema es válido para los binomios a+b,  $(a+b)^0$ , . . ,  $(a+b)^{n-1}$ , hay que demostrar el teorema para  $(a+b)^n$ . Pero los coeficientes del desarrollo de este binomio, a excepción de los extremos que son iguales a 1, son los números

$$\frac{n}{1}$$
,  $\frac{n(n-1)}{1\cdot 2}$ , ...,  $\frac{n(n-1)...2}{1\cdot 2...(n-1)}$ .

Para que todos estos números sean impares es necesario y suficiente que sean impares los números de los extremos, los cuales son precisamente iguales a n, y también que sean impares todos los números que se obtienen al borrar los factores impares de los númeradores y denominadores de los números restantes. Pero, haciendo  $n=2n_1+1$ , estos números se pueden expresar como los términos de la sucesión

$$\frac{n_1}{1}$$
,  $\frac{n_1(n_1-1)}{1\cdot 2}$ , ...,  $\frac{n_1(n_1-1)...2}{1\cdot 2...(n_1-1)}$ .

Mas éatos, como  $n_1 < n$ , son impares cuando, y sólo cuando,  $n_2$  es de la forma  $2^k - 1$ , es decir, cuando n es de la forma  $2 (2^k - 1) + 1 = 2^{k+1} - 1$ .

#### Respuestas a las preguntas del capitulo li

i, a. En la ordenada del punto de la curva y=f(x) cuya abscisa es x, hay [f(x)] puntos enteros de la región indicada

b. La igualdad Indicada se deduce de la igualdad  $T_1 + T_2 = T$ . donde  $T_1$ ,  $T_2$ , T denotan la cantidad de puntos enteros en las regiones

$$\begin{aligned} &0 < x < \frac{Q}{2} \,, &\quad 0 < y < \frac{P}{Q} \, x \,. \\ &0 < y < \frac{P}{2} \,, &\quad 0 < x < \frac{Q}{P} \, y \,. \\ &0 < x < \frac{Q}{2} \,, &\quad 0 < y < \frac{P}{2} \,. \end{aligned}$$

c. La igualdad indicada se deduce de la igualdad

$$T = 1 + 4 (T_1 + T_2 + T_3 - T_4),$$

donde  $T_1,\ T_2,\ T_3,\ T_4$  denotan la cantidad de puntos enteros en las regiones

$$x = 0, \qquad 0 < y < r;$$

$$0 < x \le \frac{r}{\sqrt{2}}, \qquad 0 < y \le \sqrt{r^2 - x^2};$$

$$0 < y \le \frac{r}{\sqrt{2}}, \qquad 0 < x \le \sqrt{r^2 - y^2},$$

$$0 < x \le \frac{r}{\sqrt{2}}, \qquad 0 < y \le \frac{r}{\sqrt{2}}.$$

d. La igualdad indicada se deduce de la igualdad  $T=T_1+T_2-T_3$  donde  $T_1,\ T_2,\ T_3$  denotan la cantidad de puntos enteros en las regiones

$$0 < x < \sqrt{n_i} \qquad 0 < y < \frac{n}{x},$$

$$0 < y < \sqrt{n_i}, \qquad 0 < x < \frac{n}{y};$$

$$0 < x < \sqrt{n_i}, \qquad 0 < y < \sqrt{n_i}$$

e En el caso de un rectángulo con los lados paralelos a los ejes coordenados, el teorema es evidente. En el caso de un trapecto con las bases paralelas a uno de los ejes coordenados y con un lado perpendicular a las bases, el teorema se demuestra fácilmente considerando el rectángulo que se forma al unir dos trapecios de éstos. El caso de un triángulo se reduce fácilmente al caso del trapecio indicado. Del caso del triángulo no es difícil pasar también al caso general, observando que un poligono con una cantidad de vértices mayor que 3 se puede dividir en dos poligonos que tenga cada uno de ellos menor cantidad de vértices. Esto se puede hacer mediante un segmento rectilineo que tenga los extremos en los vértices del poligono y que cada punto del mismo, a excepción de los extremos, sea un punto interlor del poligono

 La cantidad de números enteros positivos, no superiores a π, es igual a [π]. Cada uno de ellos se expresa de un modo único en la forma xêm, donde ê es un entero positivo, a cada x dado corresponden

$$\left[\begin{array}{c} m \\ \hline n \\ \end{array}\right]$$
 números de tal forma

8. Demostremos que las condiciones indicadas son necesarias. El número de valores x que cumplen la condición  $[\alpha x] \leqslant N$  se puede expresar en la forma  $\frac{N}{\alpha} + \lambda$ ;  $0 \leqslant \lambda < \frac{1}{\alpha}$ , y el número de valores y que cumplen la

condición  $|\beta y| \leqslant N$  se puede expresar en la forma  $\frac{N}{\beta} + \lambda_1$ ,  $0 \leqslant \lambda_1 < \frac{1}{\beta}$ .

De la igualdad  $\frac{N}{\alpha} + \lambda + \frac{N}{\beta} + \lambda_1 = N$ , dividiendo por N y pasando al llimite para  $N \rightarrow \infty$ , obtenemos  $\frac{1}{\alpha} \rightarrow \frac{1}{\beta} = 1$ . Si  $\alpha$  fuese racional,  $\alpha = \frac{a}{b}$  (a > b > 0), de la última igualdad obtendríamos que  $[\alpha b] = \frac{a}{b}$ 

=  $(\beta (a-b))$  Por lo tanto, or y  $\beta$  no pueden ser racionales. Supongamos que se cumplen las condiciones indicadas. Ses e un número

natural. Sum  $x_0 = \frac{c}{ct} + \xi$  e  $y_0 = \frac{c}{p} + \eta$  los menores números enteros

que cumpien las condiciones  $x_0>\frac{c}{\alpha}$ ,  $y_0>\frac{c}{\beta}$ . Es obvio que [ $\alpha x$ ] no es igual a c si x no es igual a  $x_0$ , y ( $\beta y$ ) no es igual a c si y no es igual a  $p_0$ ; además,  $0<\xi<1$ ,  $0<\eta<1$ ,  $\alpha\xi$  y  $\beta\eta$  son irracionales.

Como  $x_0 + y_0 = c + \xi + \eta$ , se tiene  $\xi + \eta = 1$ ,  $\frac{\alpha \xi}{\alpha} + \frac{\beta \eta}{\beta} = 1$ . Por lo tanto, uno y sólo uno de los números  $[\alpha x_0]$  y  $[\beta y_0]$  es igual a c.

4.a. Las diferencias mencionadas, para  $\{\alpha x_t\} > 0$  son iguales a

 $\{ax_1\}, \{a(x_1-x_1)\}, \ldots, \{a(x_t-x_{t-1})\}, \{-ax_t\}.$ 

Estas no son negativas, su suma es igual a 1, la cantidad de ellas es igual a t+t. Por lo tanto, al menos una de estas diferencias no es superior a  $\frac{1}{t+1} < \frac{1}{\tau}$ . Pero ésta tiene la forma  $\{\alpha x'\} = \alpha x' - y'$ , donde x' es un número entero que cumple la condición  $0 < |x'| < \tau$  y  $y' = \{\alpha x'\}$ . Por consiguiente, designando con la tetra h el número l h el modo que sea hx' > 0, se tiene  $|\alpha hx' - hy'| < \frac{1}{\tau}$ . De aqui, designando con las letras Q y P los cocientes que se obtienen al dividir hx' y hy' por  $\{hx', hy'\}$ , resulta

$$|\alpha Q - P| < \frac{1}{\tau}; \quad 0 < Q \leqslant \tau,$$

de donde se deduce el teorema mencionado en la pregunta.

b. Haclendo  $t_1 = [\tau_1], t_2 = [\tau_2], \dots, t_k = [\tau_k]$  y suponiendo que  $x_1, x_k, \dots, x_k$  recotren los valores

$$x_1 = 0, t_1, \ldots, t_k; x_k = 0, t_1, \ldots, t_k; \ldots; x_k = 0, t_1, \ldots, t_k,$$

consideramos la sucesión formada por los números  $\{\alpha_1x_1+\alpha_2x_3+\ldots, +\alpha_hx_h\}$  y el número 1, dispuestos en orden no decreciente. Formando las diferencias de los números consecutivos de esta sucesión, se obtienen  $(t_1+1)(t_2+1)\ldots(t_h+1)$  diferencias. Al menos una de éstas no es superior a

$$\frac{1}{(t_1+1)(t_2+1)\dots(t_k+1)} < \frac{t}{\tau_1\tau_0\dots\tau_k}.$$

Pero dicha diferencia tiene la forma  $(\alpha_1x_1''+\alpha_2x_3'+\ldots+\alpha_kx_k')$ , donde  $x_1', x_2', \ldots, x_k'$  son números enteros que cumplen las condiciones  $|x_1'| < < \tau_1, |x_k'| < \tau_3, \ldots, |x_k'| < \tau_k, y$  no son simultáneaments iguales e cero. Hactendo  $(\alpha_1x_1'+\alpha_2x_3'+\ldots+\alpha_kx_k')=y'$  y designando con los símbolos  $\xi_1, \xi_2, \ldots, \xi_k, \eta$  los cocientes que se obtienen al dividir  $x_1', x_2', \ldots, x_k'$  y por  $(x_1'x_2', \ldots, x_k', y')$ , resulta

$$|\alpha_1\xi_1+\alpha_2\xi_2+\ldots+\alpha_k\xi_k-\eta|<\frac{1}{\tau_1\tau_2\ldots\tau_k},$$

lo cual demuestra el teorema indicado en la pregunta.

5. So there  $\alpha = cq + r + \{\alpha\}; \ 0 < r < c$ ,

$$\left[\frac{|\alpha|}{c}\right] = \left[q + \frac{r}{c}\right] = q, \quad \left[\frac{\alpha}{c}\right] = \left[q + \frac{r + \{a\}}{c}\right] = q.$$

**6. a.** Se tiene  $[\alpha+\beta+\ldots+\lambda]=[\alpha]+[\beta]+\ldots+[\lambda]+[(\alpha)+(\beta)+\ldots+(\lambda)]$ ....+ $\{\lambda\}$ 

b. El número primo o figura en ni, al, ..., Il con los exponentes

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots + \left[\frac{a}{p}\right] + \left[\frac{a}{p^2}\right] + \dots + \left[\frac{t}{p}\right] + \left[\frac{t}{p^2}\right] + \dots$$

Además

$$\left[\frac{n}{p^{2}}\right] > \left[\frac{a}{p^{2}}\right] + \dots + \left[\frac{l}{p^{2}}\right].$$

 Suportiendo que existe un número a con las propiedades indicadas, representémosio en la forma

$$a = q_h p^{h+1} + q_{h-1} p^h + \ldots + q_1 p^2 + q_0 p + q';$$

$$0 < q_h < \rho, \ 0 \leqslant q_{h-1} < \rho, \ \dots, \ 0 \leqslant q_1 < \rho, \ 0 \leqslant q_0 < \rho, \ 0 \leqslant q' < \rho.$$

Según b, 🐧 i, tiene que ser

$$h = q_h u_h + q_{h-1} u_{h-1} + \dots + q_1 u_1 + q_0 u_0$$

Por otra parte, para cualquier s = 1, 2, ..., m, as tiene

$$q_{a-1}u_{a-1} + q_{a-2}u_{a-3} + \ldots + q_1u_1 + q_0u_0 < u_a.$$

Por lo tanto, la última expresión de h tiene que coincidir por completo con la señalada en la pregunta.

8, a. Sea  $x_1$  un entero,  $Q \leqslant \alpha \leqslant \beta \leqslant R$ ,  $x_1 \leqslant \alpha \leqslant \beta \leqslant x_1 + 1$ . Integrando por partes, se obtiene

$$-\int_{a}^{a} f(x) dx = \int_{a}^{a} \rho'(x) f(x) dx =$$

$$= p(\beta) l(\beta) - p(\alpha) l(\alpha) - \sigma(\beta) l'(\beta) + \sigma(\alpha) l'(\alpha) + \int_{\alpha}^{\beta} \sigma(x) l''(x) dx.$$

En particular, para  $Q \leqslant x_1, x_1 + 1 \leqslant R$ , pasando al limite se tiene

$$-\int_{0}^{x_1+1} f(x) dx = -\frac{1}{2} \int_{0}^{x_1+1} (x_1+1) \cdot \frac{1}{2} \int_{0}^{x_1+1} \sigma(x) f''(x) dx.$$

La formula indicada se obtiene shora sin dificultad.

b. Escribiendo la fórmula de la pregunta a en la forma

$$\sum_{Q < x \leq R} f(x) = \int_{0}^{R} f(x) dx - \int_{0}^{Q} f(x) dx + \rho(R) f(R) - \rho(Q) f(Q) - \sigma(R) f(R) + \sigma(Q) f'(Q) + \int_{0}^{\infty} \sigma(x) f''(x) dx - \int_{0}^{\infty} \sigma(x) f''(x) dx.$$

nos convencemos de que la fórmula indicada es justa.

c. Aplicando el resultado de la pregunta b, hallamos

$$=C+n\ln n-n+\frac{1}{2}\ln n+\int\limits_{-\infty}^{\infty}\frac{\sigma\left(x\right)}{x^{2}}\,\mathrm{d}x=n\ln n-n+O\left(\ln n\right).$$

9, a, c) Se tiene (b, § 1)

$$\ln ([n]!) = \sum_{p \le n} \left( \left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \dots \right) \ln p. \tag{1}$$

Aqui el segundo miembro representa la suma de los valores de la función  $\ln \rho_s$  extendida a los puntos enteros  $(\rho, s, u)$  con valores primos  $\rho$  de la región  $\rho > 0$ , s > 0,  $0 < u < \frac{n}{\rho^a}$ . La parte de la suma que corresponde a unos valores s y u dados, es igual a  $\theta \left( \sqrt[4]{\frac{n}{u}} \right)$ ; la parte que corresponde a un valor dado  $u_s$  es igual a  $\psi \left( \frac{n}{u} \right)$ .

β) Aplicando para  $n \gg 2$  el resultado de la pregunta α), se tiene

$$\ln \left( (n)! \right) - 2 \ln \left( \left\lceil \frac{n}{2} \right\rceil \right) \right) =$$

$$= \psi(n) - \psi\left( \frac{n}{2} \right) + \psi\left( \frac{n}{3} \right) - \psi\left( \frac{n}{4} \right) + \dots > \psi(n) - \psi\left( \frac{n}{2} \right).$$

Haciendo  $\left\lceil \frac{n}{2} \right\rceil = m$ , de aquí hallamos que  $\{\{n\} = 2m, \text{ o } \{n\} = 2m+1\}$ 

$$\psi(n) \quad \psi\left(\frac{n}{2}\right) < \ln\frac{(2m+1)!}{(m!)^2} < \\ < \ln\left(2^m\frac{3\cdot 5\,\ldots\,,\,(2m+1)}{1\cdot 2\,\ldots\,m}\right) < \ln\left(2^m3^m\right) < n. \\ \psi(n) = \psi(n) \quad \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{2}\right) - \psi\left(\frac{n}{4}\right) + \\ + \psi\left(\frac{n}{4}\right) - \psi\left(\frac{n}{8}\right) + \ldots < n + \frac{n}{2} + \frac{n}{4} + \ldots = 2n.$$

 γ) Se tiene (la solución de la pregunta β) y el resultado de la pregunta 8, c)

$$\begin{aligned} & \psi(n) - \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) - \psi\left(\frac{n}{4}\right) + \dots = \ln\frac{\lfloor n \rfloor!}{\left(\left\lceil \frac{n}{2} \right\rfloor!\right)^{2}} = \\ & = \lfloor n \rfloor \ln \lfloor n \rfloor - \lfloor n \rfloor - 2\left\lfloor \frac{n}{2} \right\rfloor \ln \left\lfloor \frac{n}{2} \right\rfloor + 2\left\lfloor \frac{n}{2} \right\rfloor + O(\ln n) = \\ & = n \ln 2 + O(\ln n). \end{aligned}$$

Por otra parte, para a > 2 obtenemos (pregunta 8))

$$\begin{array}{c} \Theta\left(\sqrt[n]{n}\right) - \Theta\left(\sqrt[n]{\frac{n}{2}}\right) + \\ + \Theta\left(\sqrt[n]{\frac{n}{3}}\right) - \begin{cases} <2\sqrt[n]{n} \text{ stempre} \\ = 0 \text{ st } s > \tau; \ \tau = \left[-\frac{\ln n}{\ln 2}\right] \end{cases} \end{array}$$

Por lo tanto

$$0 \leqslant \psi(n) - \psi\left(\frac{n}{2}\right) + \psi\left(\frac{n}{3}\right) - \psi\left(\frac{n}{4}\right) + \dots - \\ - \left(\Theta(n) - \Theta\left(\frac{n}{2}\right) + \Theta\left(\frac{n}{3}\right) - \Theta\left(\frac{n}{4}\right) + \dots\right) <$$

$$< 2\sqrt{n} + 2\sqrt[3]{n} + 2\sqrt[4]{n} + 2\sqrt[4]{n} + \dots + 2\sqrt[4]{n} < 2(\sqrt{n} + \sqrt[4]{n}) = O(\sqrt{n}).$$

b. Se deduce de la Igualdad (1), de la designaldad de la pregunta a, β) y de la igualdad de la pregunta 8, c.

c. Para m suficientemente grande, de la igualdad de la pregunta b, se tlene

$$\sum_{m 1.$$

Si para todos los pares  $ho_n,\ 
ho_{n+1}$  que cumplen la condición  $m<
ho_n<$  $< p_{n+1} < m^2$  so verillease la designaldad  $p_{n+1} > p_n$   $(1+\epsilon)$ , resultaria

$$\sum_{n=0}^{\infty} \frac{4}{m(1+\epsilon)^n} > 1.$$

lo cual es imposible para valores suficientemente grandes de m-

d. Evidentemente, es sufficiente considerar solamente el caso en que n es entero.

Haciendo  $\gamma(r) = \frac{\ln r}{r}$  si r es primo y  $\gamma(r) = 0$  si r = 1 o si r es compuesto, se tiene (pregunta b)

$$\gamma(1) + \gamma(2) + \ldots + \gamma(r) = \ln r + \alpha(r); \quad |\alpha(r)| < C_1.$$

donde  $C_i$  es una constante. De aquí, para r > 1

$$\sum_{0 
$$T_2 = \sum_{1 < r \le n} \frac{\alpha(r) - \alpha(r - 1)}{(r - 1)}.$$$$

$$T_1 = \sum_{1 < r \le n} \frac{\alpha(r) - \alpha(r-1)}{\ln r}.$$

Se tiene (8, b)

$$T_1 = \sum_{1 < r \le n} \frac{1}{r \ln r} + \sum_{1 < r \le n} \left( \frac{1}{2r^2 \ln r} + \frac{1}{3r^3 \ln r} + \dots \right) =$$
$$= C_2 + \ln \ln n + O\left( \frac{1}{\ln n} \right),$$

donde C2 es una constante. Luego hallamos

$$T_2 = \alpha (2) \left( \frac{1}{\ln 2} - \frac{1}{\ln 3} \right) + \dots$$

$$\dots + \alpha (n - 1) \left( \frac{1}{\ln (n - 1)} - \frac{1}{\ln n} \right) + \frac{\alpha (n)}{\ln n},$$

de donde se deduce que

$$T_2 = C_3 + O\left(\frac{1}{\ln n}\right),$$

donde  $C_3$  es la suma de la serie absolutamente convergente

$$\alpha \left(2\right) \left(\frac{1}{\ln 2} - \frac{1}{\ln 3}\right) + \alpha \left(3\right) \left(\frac{1}{\ln 3} - \frac{1}{\ln 4}\right) + \dots$$

e. Se tiene

$$\ln \prod_{p \le n} \left( 1 - \frac{1}{\rho} \right) = -\sum_{p \le n} \frac{1}{\rho} - \sum_{p \le n} \left( \frac{1}{2\rho^2} + \frac{1}{3\rho^3} + \dots \right) =$$

$$= C' + \ln \ln n + O\left( \frac{1}{\ln n} \right),$$

donde C' es una constante, De squí, haciendo  $C'=\ln C_0$ , obtenemos la igualdad indicada

f Haciendo n = [1,5 s ln s] y representando con la notación  $\pi$  (n) la cantidad de números primos que no son superiores a n, de la igualdad de la pregunta 0, a,  $\gamma$ ) deducimos (C es una constante positiva)

$$n(n) > \frac{n \ln 2 - C \sqrt{n}}{\ln n},$$

lo cual es mayor que  $s_1$  si  $s_0$  se ha elegido suficientemente grande. De aqui se deduce que, si  $s \gg s_0$ , el número  $p_a$  está comprendido entre los números primos que no son superiores a n

g. Sean  $q_1, q_2, \dots, q_n$  los divisores primos distintos del número a. Hallamos: 2, 3, 4, ...,  $(s+1) \leqslant a$ , de donde (pregunta 8, c)

$$(s+1) \ln (s+1) + O(s+1) \leqslant a, s=0 (in a)$$

Por lo tanto (preguntas e y !)

$$\frac{a}{\Psi(a)} = \frac{1}{\left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdot \cdot \cdot \left(1 - \frac{1}{q_3}\right)} \le \frac{1}{\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) \cdot \cdot \cdot \left(1 - \frac{1}{p_3}\right)} = O\left(\ln p_s\right) = O\left(\ln \ln a\right).$$

10, a. Se deduce de c. 5 2.

b Como  $\theta$  (1)  $\psi$  (1) = 1, se cumple la condición 1, a, § 2 para la función  $\theta$  (a) Sea  $a=a_1a_2$  una de las descomposiciones de a en dos lactores, primos entre si. Se tiene

$$\sum_{d_1 \setminus a_1} \sum_{d_2 \setminus a_2} \theta (d_1 d_2) = \psi (a) = \psi (a_1) \psi (a_2) = \sum_{d_1 \setminus a_1} \sum_{d_2 \setminus a_3} \theta (d_1) \theta (d_2). \quad (1)$$

Si se cumple la condición 2, a, § 2 para todos los productos menores que a, entonces, para  $d_1d_2 < a$  se tiene  $\theta$   $(d_1d_2) = \theta$   $(d_1)$   $\theta$   $(d_3)$ , y según la igualdad (1) resulta  $\theta$   $(a_1a_3) = \theta$   $(a_1)$   $\theta$   $(a_2)$ , es decir, también se cumple la condición 2, a, § 2 para todos los productos  $a_1a_3$  que son iguales a a. Mas la condición 2, a, § 2 se cumple para el único producto  $1 \cdot 1$ , igual a 1. Por consiguiente, ésta se cumple también para todos los productos.

11. a. Sea m>1; para cada  $x_m$  dado que sea div.sor de u, la ecuación indeterminada  $x_1$ , .  $x_{m-1}x_m=a$  admite  $x_{m-1}\left(\frac{a}{x_m}\right)$  soluciones. Por esto,

$$\tau_{m}\left(a\right):=\sum_{x_{m}\searrow a}\tau_{m-1}\left(\frac{a}{x_{m}}\right),$$

pero cuando  $x_{ns}$  recorre todos los divisores del número a, el número  $d = \frac{a}{x_m}$  recorre en orden inverso los mismos divisores. Por consiguiente,

$$\tau_m(a) = \sum_{a > a} \tau_{m-1}(a).$$

Por lo tanto (pregunta 10, a), si el teorema subsiste para la función  $\tau_{m-1}(a)$ , entonces también subsiste para la función  $\tau_m(a)$ . Pero el teorema es válido para la función  $\tau_t(a) = 1$ . Esto significa que el teorema siempre es válido.

b. Si el teorema subsiste para la función  $\tau_m(\rho^2)$ , se tiene

$$\tau_{m+1}(p^{\alpha}) = \sum_{s=0}^{\infty} \tau_{m}(p^{s}) = \sum_{s=0}^{\infty} \frac{(s+1)(s+2)\dots(s+m-1)}{1\cdot 2\dots(m-1)} = \frac{(\alpha+1)(\alpha+2)\dots(\alpha+m)}{1\cdot 2\dots m}$$

Por consiguiente, el teorema subsiste también para la función  $\tau_{m+1}(\rho^{th})$  Pero el teorema es vátido para la función  $\tau_{1}(\rho^{th})$  {evidentemente, igual a  $\frac{\alpha+1}{1}$  Por lo tanto, siempre es válido.

c. Supongamos que  $s = me_1$ ,  $e_1 = 2\eta$ , y que  $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$  es la descomposición canónica del número a, donde p<sub>11</sub>, ..., p<sub>k</sub> están dispuestos en orden creciente. Para la junción  $\tau_a(a) = \tau(a)$  se tiene

$$\frac{\tau(a)}{a^\eta} \leqslant \frac{\alpha_1+1}{2^{\alpha_1\eta}} \cdot \frac{\alpha_2+1}{3^{\alpha_2\eta}} \cdot \cdot \cdot \cdot \frac{\alpha_k+1}{(k+1)^{\alpha_k\eta}}.$$

Suponiendo, para simplificar los razonamientos, que  $\epsilon < 1$ , nos convencemos de que cada uno de los factores que figuran en el segundo miembro es menor que  $\frac{1}{n}$ ; los factores  $\frac{\alpha_{r-1}+1}{\alpha_{r-1}\eta}$  que cumplen la

condición  $r > 2^{\frac{1}{\eta}}$  son menores que 1. Por lo tanto, haciendo

$$C = \left(\frac{1}{\eta}\right)^{\frac{1}{2\eta}}$$
, hallamos

$$\frac{\tau(a)}{a^{\eta}} < C$$
,  $\lim_{\alpha \to \infty} \frac{\tau(a)}{a^{\varepsilon_1}} < \lim_{\alpha \to \infty} \frac{C}{a^{\eta}} = 0$ .

Si m>2, evidentemente, se tiene  $\tau_m(a) \leqslant (\tau\{a\})^m$ . Por ello

$$\lim_{a\to\infty}\frac{\tau_m\left(a\right)}{a^a}\leqslant\lim\left(\frac{\tau\left(a\right)}{a^{\epsilon_k}}\right)^m=0.$$

d. Los sistemas de valores  $x_1, \ldots, x_m$  que satisfacen a la desigualdad indicada los dividimos en [n] clases con los números de orden 1, 2, ... ..., [n] A la clase del número de orden a referimos los sistemas que cumplen la condición  $x_1$ .  $x_m = a$ , la cantidad de sistema de éstos es gual a Tm (a).

12. Si R(s) > 1, la serie que exprese  $\zeta(s)$  es absolutamente convergente Por lo tanto

$$(\zeta(s))^m = \sum_{n_1=1}^{\infty} \cdot \cdot \cdot \cdot \sum_{n_m=1}^{\infty} \frac{1}{(n_1 \dots n_m)^s} \cdot$$

que cumplen la condición na . nm -n. es igual a tm (n).

13, a. Si R(s) > 1, el producto  $P = \prod_{p} \frac{1}{1 - \frac{1}{\rho^p}}$  es absolutamente

convergente Como  $\frac{1}{1-\frac{1}{p^s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \dots$ , para N > 2 se

tiene

$$\prod_{p \leqslant N} \frac{1}{1 - \frac{1}{n^p}} = \sum_{0 < n \leqslant N} \frac{1}{n^s} + \sum' \frac{1}{n^s},$$

donde en la segunda suma del segundo miembro n recorre solamente los números que son superiores a N. Pasando al límite para  $N \ne \infty$ , en el primer miembro resulta P, en la primera suma del segundo miembro resulta  $\zeta$  (s), y en la segunda cero.

b. Sez N > 2 Supontendo que no hay números primos distintos de  $p_1, \dots, p_k$ , obtenemos (compárese con la solución de la pregunta a)

$$\prod_{j=1}^{K} \frac{1}{1 - \frac{1}{p_j}} \ge \sum_{0 < n \le N} \frac{1}{n}.$$

Como la serie armónica  $1 + \frac{1}{2} + \frac{1}{3} + \dots$  es divergente, para N suffcientemente grande, esta desigualdad es imposible.

c. Suponiendo que no hay números primos distintos de  $p_1,\ldots,p_k,$  obtenemos (pregunto a)

$$\prod_{i=1}^{A} \frac{1}{1 - \frac{l}{\rho_{1}^{A}}} = \zeta(2).$$

Como el número  $\zeta(2) = \frac{R^2}{6}$  es irracional, esta igualdad es imposible.

14. Si R(s) > 1, el producto inflinito para  $\zeta(s)$  de la pregunta 13, a es absolutamente convergente. Por lo tanto

$$\ln \zeta(s) \approx \sum_{n} \left( \frac{1}{\rho^{n}} + \frac{1}{2\rho^{2s}} + \frac{1}{3\rho^{2s}} + \dots \right),$$

donde p recorre todos los números primos. Derivando, hallamos

$$\frac{\zeta'(s)}{\zeta(s)} = \sum_{n} \left( \frac{-\ln \rho}{\rho^4} - \frac{\ln \rho}{\rho^{2s}} - \frac{\ln \rho}{\rho^{3s}} - \cdots \right) = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^4}.$$

Sea N > 2. Aplicando el teorema e, ♣ 3, se tiene

$$\prod_{\mathbf{p} \leq N} \left( 1 - \frac{1}{\rho^{\mathbf{p}}} \right) = \sum_{\mathbf{0} < \mathbf{n} \leq N} \frac{\mu(\mathbf{n})}{n^{\mathbf{a}}} + \sum_{\mathbf{i}} \frac{\mu(\mathbf{n})}{n^{\mathbf{a}}}.$$

donde en la segunda suma del segundo miembro n recorre solamente los números que son mayores que N. Pasando al límite para  $N \to \infty$  se obtiene la identidad indicada

16. a. Apliquemos d, § 3 al caso

$$\delta = \{1, 2, \dots, [n], f = \{1, 1, \dots, [n]\}$$

Entonces, evidentemente, S' = 1 Por otra parte,  $S_d$  representa el número de valores ò que son multiplos de d, es decir, es igual a  $\left[\frac{n}{d}\right]$ 

b.  $\alpha$ ) El segundo miembro de la igualdad de la pregunta a expresa la suma de los valores de la función  $\mu$  (d), extentida a los puntos enteros

(d, u) de la región d > 0,  $0 < u \leqslant \frac{\pi}{d}$  La parte de esta suma que co-

rresponde a un u dado, es igual a  $M\left(\frac{n}{\mu}\right)$ .

 β) La igualdad Indicada se obtiene restando término a término las igualdades

$$M(n) + M\left(\frac{n}{2}\right) + M\left(\frac{n}{3}\right) + M\left(\frac{n}{4}\right) + \dots = 1,$$

$$2M\left(\frac{n}{2}\right) + \qquad \qquad 2M\left(\frac{n}{4}\right) + \dots = 2.$$

c. Supongamos que  $n_1=\{n\}$ ,  $\delta_1$ ,  $\delta_3$ , ...,  $\delta_n$  se definen por la condición.  $\delta_d$  es el mayor entero cuya t-èsima potencia es un divisor de s,  $f_d=1$ . Entonces  $S'=T_{l,n}$ ,  $S_d$  es igual a la cantidad de números, no superiores a n, que son múltiplos de  $d^l$ , o sea,  $S_d=\left\lceil\frac{n}{d^d}\right\rceil$ . De aquí resulta la expresión indicada para  $T_{l,n}$ 

En particular, como  $\zeta$  (2) =  $\frac{\pi^0}{6}$ , para la cantidad  $T_{2,\,n}$  de números que no son superiores a n y que no son divisibles por el cuadrado de un entero, superior a 1, se tiene

$$T_{2, n} = \frac{6}{n^2} n + O(\sqrt{n}).$$

17, a. La igualdad indicada se obtiene de d, § 3, haciendo

$$\theta_1 = (x_0, a), \quad f_0 = f(x_0)$$

b. La igualdad indicada se obtiene de d. 6 3, haciendo

$$\delta_a = (x_1^{(a)}, \ldots, x_h^{(a)}), \quad f_a = f(x_1^{(a)}, \ldots, x_h^{(a)}).$$

c. Aplicando d, § 3 al caso

$$\delta = \delta_1, \ \delta_{3_1}, \dots, \delta_{\tau},$$

$$l = F\left(\frac{a}{\delta_1}\right), \quad F\left(\frac{a}{\delta_2}\right), \dots, F\left(\frac{a}{\delta_{\tau}}\right),$$

donde en la primera fila vienen escritos todos los divisores del número a, se tiene

$$S' = F(a), \quad S_d = \sum_{D > \frac{a}{d}} F\left(\frac{a}{dD}\right) = G\left(\frac{a}{d}\right).$$

d. La igualdad indicada se deduce de

$$P' = \int_{0}^{L} \frac{\mu(d)}{h} \sum_{\substack{j=1 \ j \neq 0}} \mu(d) \sum_{\substack{j=1 \ j \neq 0}} \mu(d) \cdots \int_{0}^{L} \frac{1}{h} h(d).$$

16, a. Apliquemos el teorema de la pregunta 17, a, suponiendo que x recorre los números 1, 2, ..., a y tomando  $f(x) = x^m$ . Entonces

$$S' = \psi_m(a)$$
,  $S_d = d^m + 2^m d^m + \ldots + \left(\frac{a}{d}\right)^m d^m = d^m \sigma_m\left(\frac{a}{d}\right)$ .

b. Se tiene

$$\psi_1(a) = \sum_{d \geq a} \mu(d) \left( \frac{a^3}{2d} + \frac{a}{2} \right) = \frac{a}{2} \varphi(a)$$

El mismo resultado se puede obtener más fácilmente. Escribamos los números de la sucesión I, . . , a que son primos con a, primero en orden creciente y luego en orden decreciente. La suma de los términos de ambas sucesiones que equidistan del origen, es igual a a; la cantidad de términos de cada sucesión es igual a o (a).

c. Se tlene

$$\begin{split} \psi_{h}\left(a\right) &= \sum_{\mathbf{B} \setminus \mathbf{o}} \mu\left(a\right) \left(\frac{a^{\mathbf{B}}}{3d} + \frac{a^{2}}{2} + \frac{a}{6} d\right) = \\ &= \frac{a^{3}}{3} \ \psi\left(a\right) + \frac{a}{6} \left(1 - \rho_{1}\right) \dots \left(1 - \rho_{h}\right). \end{split}$$

19. s. Apliquemos el teorema de la pregunta 17. a, suponiendo que x recorre los números 1, 2, . . . , [z] y tomando f(x) = 1. Entonces  $S' = T_z$ ,  $S_d$  es igual a la cantidad de números, no superiores a z, que son múltiplos de d, o sea,  $S_d = \left\lceil \frac{z}{d} \right\rceil$ .

b. Se tlene

$$T_z = \sum_{d > a} \mu(d) \frac{z}{d} + O(\tau(a)) = \frac{z}{a} \psi(a) + O(a^a).$$

c. Se deduce de la igualdad de la pregunta a.

20. Apliquemos el teorema de la pregunta 17, a, suponiendo que x recorre los números 1, 2, ..., N, donde N > a, y tomando  $f(x) = \frac{1}{x^a}$ . Entonces se obtiene

$$\sum_{\varkappa\leqslant N}'\frac{1}{\varkappa^{\mathfrak{o}}} = \sum_{\mathsf{d}\smallsetminus a}\mu\left(\mathsf{d}\right)\sum_{0<\varkappa\leqslant\frac{N}{\mathsf{d}}}\frac{1}{\mathsf{d}^{\mathfrak{o}}\varkappa^{\mathfrak{o}}} = \sum_{\mathsf{d}\smallsetminus a}\frac{\mu\left(\mathsf{d}\right)}{\mathsf{d}^{\mathfrak{o}}}\sum_{0<\varkappa\leqslant\frac{N}{\mathsf{d}}}\frac{1}{\varkappa^{\mathfrak{o}}}\;.$$

Pasando al límite para  $N \to \infty$  se obtiene la identidad indicada. 21, a. Apliquemos el teorema de la pregunta 17, b, considerando los sistemas de valores  $x_1, x_2, \ldots, x_k$  indicados en la definición de probabilidad  $P_N$  y tomando  $f(x_1, x_2, \ldots, x_k) = l$ . Entonces  $P_N = \frac{S'}{N^k}$ ,

$$S_d = \left[\frac{N}{d}\right]^h$$
, y se tiene

$$P_{N} = \frac{\sum_{d=1}^{N} \mu(d) \left[\frac{N}{d}\right]^{h}}{N^{h}} = \sum_{d=1}^{N} \frac{\mu(d)}{d^{h}} + O\left(\sum_{d=1}^{N} \frac{1}{Nd^{h-1}}\right).$$

Por lo tanto

$$P_N = (\zeta(k))^{-1} + O(\Delta);$$
  $\Delta = \frac{1}{N}$  so  $k > 2$ , 
$$\Delta = \frac{\ln N}{N} \text{ so } k = 2.$$

b. Se tiene  $\zeta(2) = \frac{\pi^2}{6}$ .

22, a. Razonamientos elementales muestran que la cantidad de puntos enteros (u, v) que hay en la región  $u^2 + v^2 \leqslant \rho^2$ ,  $\rho < 0$ , es igual a  $n\rho^3 + O(\rho)$  Apliquemos el teorema 17, b, considerando las coordenadas x, y de los puntos enteros de la región  $x^2 + y^2 \leqslant r^2$ , distintos del punto (0, 0), y haciendo f(x, y) = 1 Entonces T = S' + 1,  $S_d$  es igual a la cantidad de puntos enteros que hay en la región  $u^2 + v^2 \leqslant$ 

 $\leq \left(\frac{r}{d}\right)^{3}$ , sin contar el punto (0, 0). Por lo tanto

$$S_d = \pi \frac{r^2}{d^2} + O\left(\frac{r}{d}\right),$$

$$T = \sum_{d=1}^{\{r\}} \mu(d) \pi \frac{r^3}{d^2} + O\left(\sum_{d=1}^{\{r\}} \frac{r}{d}\right) = \frac{6}{\pi} r^2 + O(r \ln r)$$

b. Razonando Igual que anteriormente, se obtiene

$$T = \sum_{d=1}^{\lfloor r\rfloor} \mu(d) \, \frac{4}{3} \, \pi \, \frac{r^3}{d^3} + O \, \left( \sum_{d=1}^{\lfloor r\rfloor} \frac{r^2}{d^3} \right) = \frac{4\pi r^3}{3 \zeta(3)} + O \, (r^2).$$

23, a. Le cantidad de divisores d de un número  $a=\rho_1^{\alpha_1}$ .  $\rho_k^{\alpha_k}$ , que no son divisibles por el cuadrado de un entero, superior a 1, y que tienen  $\kappa$  divisores primos, es igual a  $\binom{k}{\kappa}$ ; en este caso  $\mu(d)=(-1)^k$ . Por lo tanto

$$\sum_{d \geq n} \mu(d) = \sum_{N=0}^{h} {h \choose N} (-1)^{N} = (1-1)^{h} = 0.$$

b. Supongamos que a tiene la misma forma que en la pregunta a Es suficiente considerar el caso m < k. Para la suma indicada se tienen dos expresiones

$$\sum \mu(d) = {k \choose 0} - {k \choose 1} + \dots + (-1)^m {k \choose m} =$$

$$= (-1)^m \left( {k \choose m+1} - {k \choose m+2} + \dots \right).$$

SI m es par, entonces, para  $m < \frac{k}{2}$  la primera expresión es >0, y para  $m > \frac{k}{2}$  la segunda expresión es >0. Si m es impar, entonces, para  $m < \frac{k}{2}$  la primera expresión es <0, y para  $m > \frac{k}{2}$  la segunda expresión es <0.

c. La demostración es casi igual que en d, §, 3, pero teniendo en cuenta ol resultado de la pregunta b.

d. La demostración es cast igual que en las preguntas 17, a y 17, b. 24. Supongamos que d'recorre los divisores del numero  $a \Omega(d)$  denota la cantidad de divisores primos del numero d,  $\Omega(a) = s$ . De acuerdo

a la indicación hecha en la pregunta, se tiene (suponemos que N es suficientemente grande)

$$\begin{split} \pi\left(N,\,q,\,l\right) &\leqslant \sum_{\Omega(d) \leqslant m} \mu\left(d\right) \left(\frac{N}{qd} + \theta_d\right) = T + T_0 - T_1; \quad |\theta_d| \leqslant 1. \\ &|T| \leqslant \sum_{\Omega(d) \leqslant m} 1, \quad T_0 = \frac{N}{q} \sum_{d} \frac{\mu\left(d\right)}{d}, \quad |T_4| = \sum_{\Omega(d) \geqslant m} \frac{N}{\varrho d}. \end{split}$$

Luego hallamos

$$\begin{split} |T| \leqslant \sum_{n=0}^{m} \binom{s}{n} \leqslant s^m \leqslant s^{hm} \leqslant s^{6r^{1-\alpha}} \ln r \frac{qr}{N} \frac{N}{qr} = O\left(\Delta\right), \\ T_0 = \frac{1}{q} \prod_{p \leqslant s^h} \left(1 - \frac{1}{\rho}\right) = O\left(\Delta\right). \end{split}$$

Finalmente, designando con las letras  $C_1$  y  $C_2$  unas constantes, se tiene

$$T_{1} < \frac{N}{q} \sum_{n=m+1}^{q} \sum_{\Omega(d)=n}^{q} \frac{1}{d} < \frac{N}{q} \sum_{n=m+1}^{q} \frac{\left(\frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{\rho_{0}}\right)^{n}}{n!} < \frac{N}{q} \sum_{n=m+1}^{q} \left(\frac{C_{1} + \ln r}{4 \ln r} e\right)^{n} < \frac{N}{q} \sum_{n=m+1}^{q} \left(\frac{3}{4}\right)^{n} < C_{2} \frac{N}{q} r^{-4 \ln \frac{4}{3}} = O(\Delta).$$

25. A todo divisor  $d_1$  del número a, que cumple la condición  $d_1 < \sqrt{a}$ . le corresponde un divisor  $d_2$  que cumple las condiciones  $d_3 > \sqrt{a}$ .  $d_1d_3 = a$  Ahora bien,  $\mu(d_1) = \mu(d_2)$ . Por lo tanto,

$$2\sum_{d_1}\mu(d_2) = \sum_{d_1}\mu(d_1) + \sum_{d_2}\mu(d_2) = \sum_{d > a}\mu(d) = 0$$

28. Los números d que no son divisibles por el cuadrado de un entero, superior a 1, y que satisfacen a la condición  $\psi(d) = k$ , los consideramos

a pares, de modo que en cada par figure un impar  $d_1$  y un par  $2d_1$ . Se tiene  $\mu(d_1) + \mu(2d_2) = 0$ .

27. Sean  $p_1, \ldots, p_k$  distintos números primos. Haciendo  $a \circ p_1 \ldots p_k$ , se tiene

$$\phi(a) = (p_1 - 1) \dots (p_k - 1).$$

Sin embargo, si no hublese números primos, distintos de  $p_1, \ldots, p_h$ , se tendría  $\phi(a) = 1$ .

28, a. Los números indicados se hallan entre los números sô,  $s=1,2,\ldots,\frac{a}{b}$ . Pero  $(s\delta,a)=\delta$  cuando, y sólo cuando,  $\left(s,\frac{a}{b}\right)=1$   $(e,\frac{a}{b},2,cap. 1)$ . Por lo tanto, es justa la afirmación señalada en la pregunta, y se tiene

$$a = \sum_{\delta \leq a} \varphi\left(\frac{a}{\delta}\right) = \sum_{d \leq a} \varphi\left(d\right)$$

**b**,  $\alpha$ ) Sea  $a=p_1^{\alpha_1}$  ...  $p_k^{\alpha_k}$  la descomposición canónica del número a. En virtud de a, la función  $\phi(a)$  es multiplicativa, y se tiene

$$\rho_{\mathfrak{g}}^{\alpha_{\mathfrak{g}}} = \sum_{d \, \backslash \, \mathcal{p}_{\mathfrak{g}}^{\alpha_{\mathfrak{g}}}} \phi \left( d \right), \quad \rho_{\mathfrak{g}}^{\alpha_{\mathfrak{g}} - 1} = \sum_{d \, \backslash \, \mathcal{p}_{\mathfrak{g}}^{\alpha_{\mathfrak{g}} - 1}} \phi \left( d \right), \quad \rho_{\mathfrak{g}}^{\alpha_{\mathfrak{g}}} - \rho_{\mathfrak{g}}^{\alpha_{\mathfrak{g}} - 1} := \phi \left( \rho_{\mathfrak{g}}^{\alpha_{\mathfrak{g}}} \right).$$

β) Para un entero m > 0 se tiene

$$m := \sum_{d > \infty} \varphi(d).$$

Por lo tanto

$$\varphi(a) = \sum_{d > a} \mu(d) \frac{a}{d}.$$

29. Se tiene (p recorre todos los números primos)

$$\sum_{n=1}^{\infty} \frac{\varphi(n)}{n^{s}} = \prod_{p} \left( 1 + \frac{\varphi(p)}{p^{s}} + \frac{\varphi(p^{2})}{p^{2s}} + \dots \right) = \prod_{p} \frac{1 - \frac{1}{p^{s}}}{1 - \frac{1}{n^{s-1}}} = \frac{\zeta(s-1)}{\zeta(s)}.$$

30. Se tiene

$$\varphi(1) + \varphi(2) + \dots + \varphi(n) =$$

$$= \sum_{d \ge 1} \frac{\mu(d)}{d} + 2 \sum_{d \ge 2} \frac{\mu(d)}{d} + \dots + n \sum_{d \ge n} \frac{\mu(d)}{d} =$$

$$= \sum_{d = 1}^{n} \mu(d) \left(1 + 2 + \dots + \left[\frac{n}{d}\right]\right) = \sum_{d = 1}^{n} \mu(d) \frac{n^{2}}{2d^{2}} + O(n \ln n) =$$

$$= \frac{n^{2}}{2} \sum_{d \ge 1}^{\infty} \frac{\mu(d)}{d^{2}} + O(n \ln n) = \frac{3}{n^{2}} n^{2} + O(n \ln n).$$

## Respuestas a las pregentas del capitulo ili

I, a. De

$$P = a_n (0n-1 + a_{n-1})(0n-2 + ... + a_1)$$

observando que 10 = 1 (mód. 9), se tiene

$$P = a_n + a_{n-1} + \ldots + a_1 \pmod{9}$$
.

Por consiguiente, P es un múltiplo de 3 cuando, y sólo cuando, la suma de las cifras que le representan es un múltiplo de 3, P es un múltiplo de 9 cuando, y sólo cuando, la suma indicada es un múltiplo de 9 Observando que  $10 = -1 \pmod{1}$ , se tiene

$$P = (a_1 + a_2 + ...) - (a_2 + a_4 + ...)$$
 (mod 11)

Por lo tanto, P es un múltiplo de 11 cuando, y sólo cuando, la diferencia entre la suma de las cifras que ocupan lugares impares (contando desde la derecha) y la suma de las cifras que ocupan lugares pares, es un múltiplo de 11 b. De

$$P = b_n 100^{n-1} + b_{n-1} 100^{n-2} + \dots + b_n$$

debido a que 100 🖮 -- I (mód 101), se tiene

$$P = (b_1 + b_2 + \cdots) - (b_2 + b_4 + \cdots)$$
 (mód. 101)

Por consiguiente, P es un múltiplo de 101 cuando, y sólo cuando,  $(b_1+b_3+\cdots)=(b_1+b_4+\cdots)$  es un múltiplo de 101 c. De

$$P = c_n 1 \ 000^{n-1} + c_{n-1} 1 \ 000^{n-2} + \dots + c_1$$

debido a que 1 000 - 1 (mód 37), se tiene

$$P = c_n + c_{n-1} + \dots + c_1 \pmod{37}$$

Por lo tanto, P es un múltiplo de 37 cuando, y sólo cuando,  $c_n+c_{n-1}+c_{n-1}+\ldots+c_1$  es un múltiplo de 37

Como 1000 = -1 (mód 7·11·13), se tiene  $P = (c_1 + c_2 + ...)$  ( $c_3 + c_4 + ...$ ) (mód 7·11·13).

Por ello, P es un múltiplo de uno de los números 7, 11, 13 cuando, y sólo cuando,  $(c_1 + c_3 + \cdots)$   $(c_3 + c_4 + \cdots)$  es un múltiplo de este mismo número

2. a) Cuando x recorre el sistema completo de restos respecto del módulo m, ax + b también recorre el sistema completo, el resto minimo no negativo r del número ax + b recorre los valores  $0, 1, \dots, m-1$ . De agui que

$$\sum_{x} \left\{ \frac{ax+b}{m} \right\} = \sum_{r=0}^{m-1} \frac{r}{m} = \frac{1}{2} (m-1).$$

Aplicando el resultado de la pregunta 18, b, cap. Il, se obtieñe

$$\sum_{k} \left\{ \frac{a\xi}{m} \right\} = \frac{\psi_1\left(m\right)}{m} = \frac{1}{2} \varphi\left(m\right)$$

8, a. Sea r el resto minimo no negativo del número  $ax + \{c\}$  respecto del módulo m. Se tiene

$$S = \sum_{r=0}^{m-1} \left\{ \frac{r + \Phi(r)}{m} \right\},\,$$

donde  $s \le 0$  (r)  $\le s+h$ ,  $s=\{c\}$ . Si  $m \le 2h+1$  el teorema es evidente. Por la tanto, consideraremos sólo el caso en que m>2h+1. Haciendo

$$\left\{\frac{r+\Phi(r)}{m}\right\}-\frac{r}{m}=\delta(r),$$

se tiene  $-1 + \frac{\varepsilon}{m} < \delta(r) < \frac{h+\varepsilon}{m}$  si  $r = m - [h+\varepsilon], \dots m-1, \frac{\varepsilon}{m} < \infty$ 

 $<\delta(r)<\frac{h+a}{m}$  en todos los demás casos. De aqui resulta que

$$-\{h+e\}+\epsilon \leqslant S-\frac{m-1}{2}\leqslant h+\epsilon, \quad \left|S-\frac{1}{2}m\right|\leqslant h+\frac{1}{2}.$$

b. Se tiene

$$S = \sum_{z=0}^{m-1} \left\{ \frac{az + \psi(z)}{m} \right\} :$$

$$\psi(z) = m(AM + B) + \frac{\lambda}{m}z.$$

Apliquemos el teorema de la pregunta a, haciendo  $h = \lceil \lambda \rfloor$ . Entonces se obtiene el resultado señalado.

c. Se halla

$$\sum_{s=0}^{m-1} \left\{ f(M) + \frac{az}{m} + \frac{\theta z}{m^2} + \frac{f^*(M+z_0)}{2} z^2 \right\};$$

$$0 < z_0 < m-1.$$

Aplicamos el teorema de la pregunta a, haciendo  $h=1+\frac{k}{2}$ . Entonces se obtiene el resultado indicado

4. Desarrollemos A en fracción continua. Sea  $Q_n=Q'$  el mayor de los denominadores de las fracciones reducidas, que no es superior a m Se tiene (pregunta 4, b, cap. 1)

$$A = \frac{P'}{Q'} + \frac{\theta'}{Q'm}, \quad (P', Q') = 1, \quad |\theta'| < 1.$$

De las designaldades  $m < Q_{n+1} \le (q_{n+1} + 1) \ Q_n \le CQ_n$ , donde C es una constante, a la cual no superan todos los números  $q_n + 1$ , para el mayor entero H' que cumple la condición  $H'Q' \le m$  se deduce que H' < C. Aplicando el teorema de la pregunta 3, b, se obtiene

$$\left| \sum_{x=M}^{M+H'Q'-1} (Ax+B) - \frac{1}{2} H'Q' \right| \leqslant \frac{3}{2} C.$$

Sea  $m_1 \circ m = H'Q'$  Si  $m_1 > 0$ , entonces, eligiendo los números Q'' y H'' en dependencia de  $m_1$ , del mismo modo que se eligieron antes los números Q' y H' en dependencia de  $m_1$  se obtiene

$$\sum_{x=M_1}^{M_1+H^*Q^*-1} \left| \{Ax+B\} - \frac{1}{2} H^*Q^* \right| \leq \frac{3}{2} C.$$

donde aplicamos la notación  $M_a=M_{a-1}+H^{(a)}Q^{(a)}$ . Sea  $m_2=m_1-H^aQ^a$ . Si  $m_2>0$ , entonces, de un modo semejante a lo anterior, se halla

$$\Big|\sum_{x=M_3}^{M_2+H=Q^m-1} (Ax+B) - \frac{1}{2}H^mQ^m\Big| < \frac{3}{2}C$$

etc., hasta que se llegue a un  $m_h=0$ . Entonces se obtiene  $(H'Q'+H''Q'+\ldots+H^{(h)}Q^{(h)}=m)$ 

$$\left| \sum_{n=-M}^{M+m-1} \{Ax + B\} - \frac{1}{2} m \right| < \frac{3}{2} Ck.$$

Los números Q', Q'', ,  $Q^{(k)}$  satisfacen a las condiciones  $m \gg Q' > m_1 \gg Q'' > m_1 \gg \cdots > m_{k-1} \gg Q^{(k)} \gg 1$ .

De aqui que (pregunta 3, cap  $| 1 \rangle k \sim O(\ln m)$  y, por consiguiente la formula indicada en la pregunta es cierta

5, a. Designemos con S la suma que figura en el primer miembro

See  $\tau = A^{\frac{1}{3}}$  Para  $\tau \leqslant 40$  el teorema es evidente. Por lo tanto, suponemos que  $\tau > 40$ . Tomando  $M_1 = [Q+1]$ , haliamos unos números  $a_1, m_1, \theta_1$  que cumplan las condiciones.

$$I'(M_1) = \frac{a_1}{m_2} + \frac{\theta_1}{m_2 \tau}; \quad 0 < m_1 \leqslant \tau, \quad (a_1, m_1) = 1, \quad , \theta_1 \mid < 1$$

Tomando  $M_2 = M_{1-1} m_1$ , del mismo modo hallamos los números  $a_2$ ,  $m_2$ ,  $\theta_3$ ; tomando  $M_3 = M_2 + m_3$ , hallamos los números  $a_3$ ,  $m_3$ ,  $\theta_3$ ; continuamos así hasta que se llegue a  $M_{s+1} = M_{s-1} m_s$  con la condición  $0 \le |R| - M_{s+1} < |\tau|$ . Aplicando el teorema de la pregunta 3, c, se obtiene

$$\left| S - \frac{1}{2} \left( m_1 + m_2 + \dots + m_s + [R] + 1 - M_{s+1} \right) \right| <$$

$$< s \frac{k+3}{2} + \frac{1}{2} \left( [R] + 1 - M_{s+1} \right),$$

$$\left| S - \frac{1}{2} \left( R - Q \right) \right| < s \frac{k+3}{2} + \frac{\tau + 1}{2}.$$

La fongitud del intervalo, para el cual

$$\frac{a}{m} - \frac{1}{m\tau} \leqslant f'(x) \gg \frac{a}{m} + \frac{1}{m\tau}$$

no es superior a  $\frac{2A}{m\tau}$ . Por consiguiente, con una misma fracción  $\frac{a}{m}$  están ligados  $\leqslant \frac{2A}{m^2\tau} + 1$  números  $m_1, m_2, \dots, m_4$ . Sean  $a_1$  y  $a_2$  el valor mínimo y máximo de a que corresponden a un m dado. Se tiene

$$\frac{a_2-a_1}{m}-\frac{2}{m\tau} \leqslant \frac{k(R-Q)}{A}; \quad a_2-a_1+1 \leqslant \frac{k(R-Q)m}{A}+1.05.$$

Por consiguiente, con el m dado están ligados

$$< \left(\frac{2A}{m^2\tau} + 1\right) \left(\frac{k(R-Q)m}{A} + 1.05\right) = \frac{k(R-Q)}{\tau} \left(\frac{2}{m} + \frac{m}{\tau^2}\right) \left(\frac{2A}{m^2\tau} + 1\right) 1.05$$

números  $m_1$ ,  $m_2$ , . . ,  $m_s$ . Sumando la última expresión respecto de todos los  $m=1, 2, \ldots, \{v\}$ , se obtiene

$$s < \frac{k(R-Q)}{\tau} \left( 2 \ln \tau + 2 + \frac{\tau^2 + \tau}{2\tau^2} + \frac{10A}{3\tau} \right), 05 < \frac{k(R-Q)}{\tau} \ln A + \frac{7}{2} \frac{A}{\tau},$$

$$\left| S - \frac{1}{2} (R-Q) \right| < 2 \frac{k^2 (R-Q)}{\tau} \ln A + 8k \frac{A}{\tau}.$$

b. Se tiene

$$\begin{split} \Big| \sum_{Q < x \le R} \{I(x) + 1 - \sigma\} - \frac{1}{2} (R \cdot Q) \Big| < \Delta, \\ \Big| \sum_{Q < x \le R} \{I(x)\} - \frac{1}{2} (R - Q) \Big| < \Delta. \end{split}$$

de donde, haciendo  $\delta(x) = \{f(x) + 1 - \sigma\} - \{f(x)\}, hallamos$ 

$$\Big|\sum_{Q < x \in R} \delta(x)\Big| < 2\Delta.$$

Mas, si  $\{f(x)\} < \sigma$  so there  $\delta(x) = 1 - \sigma$ , y si  $\{f(x)\} > \sigma$  so there  $\delta(x) = -\sigma$ . Por lo tanto,  $|\{1 - \sigma\} \psi(\sigma) - \sigma(R - Q - \psi(\sigma))| < 2\Delta$ , de donde se obtiene la fórmula indicada.

6, a. Apliquemos la fórmula de la pregunta 1, c, cap. II. Haciendo  $I(x) = \sqrt{r^2 - x^2}$ , en el intervalo  $0 \le x \le \frac{r}{\sqrt{r^2}}$  se tiene

$$f'(x) = -\frac{x}{\sqrt{r^2 - x^2}}, \quad f''(x) = \frac{-r^2}{(r^2 - x^2)^{\frac{3}{2}}}, \quad \frac{1}{r} < |f''(x)| < \frac{\sqrt{8}}{r},$$

Por lo tanto (pregunta 8, a, cap. II, pregunta 5, a)

$$T = 4r + 8 \int_{0}^{\frac{r}{\sqrt{2}}} \sqrt{r^{2} - x^{2}} dx + 8\rho \left(\frac{r}{\sqrt{2}}\right) \frac{r}{\sqrt{2}} - 8\rho (0) \cdot r - 4 \frac{r}{\sqrt{2}} - 4 \frac{r^{2}}{2} + 8 \frac{r}{\sqrt{2}} \left\{\frac{r}{2}\right\} + O(r^{\frac{2}{3}} \ln r) = \pi r^{2} + O(r^{\frac{2}{3}} \ln r).$$

b. Se tiene (preguntas II, d y I, d, cap. II)

$$\tau(1) + \tau(2) + \dots + \tau(n) = 2 \sum_{0 < x \le V \tilde{n}} \left[ \frac{n}{x} \right] - [V \tilde{n}]^2.$$

Es suficiente considerar solamente el caso n > 64. Dividamos el intervalo  $X < x < \sqrt{n}$ , donde  $X = 2n^{\frac{1}{3}}$ , en  $O(\ln n)$  intervalos de la forma M < x < M', donde M' < 2M. Haciendo  $f(x) = \frac{n}{x}$ , en el intervalo M < x < M' se tiene

$$\begin{split} f'\left(z\right) &= -\frac{n}{z^{3}}\;, \quad f''\left(z\right) = \frac{2n}{z^{3}}\;, \\ &\frac{n}{4M^{3}} \ll f''\left(z\right) \ll \frac{8n}{4M^{3}}\;. \end{split}$$

De aquí que (pregunta 6, a)

$$\sum_{M < x \leqslant M'} \left\{ \frac{n}{x} \right\} = \frac{1}{2} (M' - M) + O\left(n^{\frac{1}{3}} \ln n\right),$$

$$\sum_{M < x \leqslant M'} \left\{ \frac{n}{x} \right\} = \frac{1}{2} \sqrt{n} + O\left(n^{\frac{1}{3}} (\ln n)^2\right).$$

Por otra parte (pregunta 8, b, cap. 18)

$$\sum_{0 < n \le \sqrt[n]{n}} \frac{n}{x} = En + \frac{1}{2} n \ln n + \rho \left( \sqrt[n]{n} \right) \sqrt[n]{n} + O(1).$$

Por lo tanto

$$\begin{aligned} \tau(1) + \tau(2) + \dots + \tau(n) &= 2En + n \ln n + 2p \left(\sqrt{n}\right) \sqrt{n} - \\ &- \sqrt{n} - n + 2 \sqrt{n} \left(\sqrt{n}\right) + O_{\epsilon} \left(n^{\frac{1}{3}} (\ln n)^{2}\right) = n \left(\ln n + 2E - 1\right) + \\ &+ O\left(n^{\frac{1}{3}} (\ln n)^{3}\right). \end{aligned}$$

- 7. Supongamos que el sistema es irregular y sea s el mayor número entero que cumple la condición de que 2º figura en una cantidad impar de números del sistema. Uno de estos últimos números lo sustituimos por otro menor, que contenga solamente aquellas potencias 2º que liguran en una cantidad impar de números del sistema restante. Supongamos que el sistema es regular. Un número, que sea menor que alguno de los números T de este sistema, se diferencia de T al menos en una clira en el sistema de numeración de base 2
- 8, a. Agregando el número  $H=3^n+3^{n-1}+\ldots+3+1$  a cada uno de los números, representados del modo indicado, se oblienen

los números que se pueden obtener si en la misma forma  $x_n, x_{n-1} \dots$ , ...,  $x_1, x_2$  recorren los valores 0, 1, 2, o sea, se obtienen todos los números 0, 1, ..., 2H.

b. Del modo indicado se obtienen  $m_1m_2$  . .  $m_k$  números que no son congruentes entre si respecto del módulo  $m_1m_2$  . .  $m_k$ , puesto que de

$$x_1 + m_1x_2 + m_1m_2x_3 + \dots + m_1m_3 \dots m_{k-1}x_k = x_1' + m_1x_2' + m_1m_2x_3' + \dots + m_1m_3 \dots m_{k-1}x_k' \pmod{M_1m_3 \dots m_k}$$

se halla sucesivamente

$$x_1 = x_1' \pmod{m_1}, \quad x_1 = x_1'; \quad m_1 x_2 \equiv m_1 x_2' \pmod{m_1 m_2}, \quad x_2 = x_2';$$
  
 $m_1 m_2 x_3 \equiv m_1 m_2 x_3' \pmod{m_1 m_2 m_3}, \quad x_3 = x_3',$ 

etc.

 $\Psi_i$  a. Del modo indicado se obtienen  $m_1m_2$ ...  $m_k$  números que no son congruentes respecto del módulo  $m_1m_2$ ...  $m_k$ , puesto que de

$$\begin{aligned} M_1 x_1 + M_2 x_2 + \ldots + M_h x_h &\equiv \\ &= M_1 x_1' + M_2 x_2' + \ldots + M_h x_h' \ (\text{mod. } m_1 m_2 \ldots m_h) \end{aligned}$$

resultaria que (todo  $M_f$ , distinto de  $M_a$ , es un múltiplo de  $m_d$ )

$$M_a x_a \equiv M_a x_a' \pmod{m_a}, \quad x_a \equiv x_a' \pmod{m_a}, \quad x_a = x_a'.$$

b. Del modo indicado se obtienen  $\varphi(m_1) \varphi(m_2) \dots \varphi(m_k) = \varphi(m_1 m_1 \dots m_k)$  números, los cuales, en virtud del teorema de la pregunta a, no son congruentes respecto del módulo  $m_1 m_2 \dots m_k$ , y como  $(M_1 x_1 + M_2 x_2 + \dots + M_k x_k, m_k) = (M_0 x_0, m_0) = 1$ , son primos con  $m_1 m_2 \dots m_k$ .

c. Según el teorema de la pregunta a, el número  $M_1x_1 + M_2x_2 + \dots + M_kx_k$ , donde  $x_1, x_2, \dots, x_k$  reccorren los sistemas completos de restos respecto de los módulos  $m_1, m_2, \dots, m_k$ , recorre el sistema completo de restos respecto del módulo  $m_1m_2 \dots m_k$ . Este número es primo con  $m_1m_2 \dots m_k$  cuando, y sólo cuando,  $(x_1, m_1) = \dots = (x_3, m_3) = \dots = (x_k, m_k) = 1$  De aquí que  $\emptyset$   $(m_1m_2 \dots m_k) = \dots = \emptyset$   $(m_1, m_2, \dots, m_k) = \dots = \emptyset$ 

d. Para obtener todos los números de la sucesión 1, 2, ...  $p^{\alpha}$  que son primos con  $p^{\alpha}$ , se deben borrar los números de esta sucesión que son múltiplos de p, es decir, los números p, 2p, ...  $p^{\alpha-2}p$  Por lo tanto,  $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$ . De aquí y del teorema c,  $\frac{1}{2}$  4, cap. Il se deduce inmediatamente la expresión para  $\varphi(\alpha)$ .

10, a. La primera afirmación se deduce de

$$\left\{\frac{z_t}{m_t} + \ldots + \frac{z_h}{m_h}\right\} = \left\{\frac{M_1 z_1 + \ldots + M_h z_h}{m_t}\right\};$$

la segunda se deduce de

$$\left\{ \begin{array}{l} \xi_{\frac{1}{2}} + \ldots + \frac{\xi_{h}}{m_{h}} \right\} = \left\{ \frac{M_{1}\xi_{1} + \ldots + M_{h}\xi_{h}}{m} \right\}.$$

b. Las fracciones

$$\left\{\frac{f_1\left(x_1,\ldots,w_1\right)}{m_1}+\ldots+\frac{f_k\left(x_k,\ldots,w_k\right)}{m_k}\right\}$$

coinciden con las fracciones

$$\left\{ \frac{f_1(M_1x_1 + \ldots + M_hx_h, \ldots, M_1x_2 + \ldots + M_hw_h}{m_1} + \ldots + \frac{f_h(M_1x_1 + \ldots + M_hx_h, \ldots, M_1w_2 + \ldots + M_hw_h)}{m_h} \right\}.$$

e sen, con las fracciones  $\left\{\frac{f_1\left(x,\ldots,w\right)}{m_1}+\ldots+\frac{f_h\left(x,\ldots,w\right)}{m_h}\right\}$ . De aqui se obtiene fáculmente la primera alirmación. La segunda se demuestra de un modo análogo.

11. a. Si a es un múltiplo de m, se tiene

$$\sum e^{\frac{2\pi i \cdot \frac{dx}{m!}}} = \sum_{x} 1 = m_x$$

St a no es divisible por m, se tiene

$$\sum_{x} e^{\frac{2\pi i}{m}} = \frac{e^{\frac{2\pi i}{m}} - 1}{e^{\frac{2\pi i}{m}} - 1} = 0.$$

b. Para os no entero, el primer miembro es igual a

$$\left| \frac{e^{2\pi i \alpha (M+P)} - e^{2\pi i \alpha M}}{e^{2\pi i \alpha} - 1} \right| < \frac{1}{\sec \pi \left( \alpha \right)} < \frac{1}{h \left( \alpha \right)}$$

 Según el teorema de la pregunta b, el primer m.embro no es superior a T<sub>ms</sub> donde

$$T_m = \sum_{\alpha=1}^{m-1} \frac{1}{h\left(\frac{\alpha}{m}\right)}.$$

Pero el m es impar

$$T_m < m \sum_{0 < a < \frac{m}{2a - 1}} \ln \frac{2a + 1}{2a - 1} = m \ln m.$$

y al m es par

$$T_m < \frac{m}{2} \sum_{0 < a \leqslant \frac{m}{3}} \ln \frac{2a+1}{2a-1} + \frac{m}{2} \sum_{0 < a < \frac{m}{3}} \ln \frac{2a+1}{2a-1} < m \ln m.$$

Como  $\frac{1}{2} - \frac{1}{3} = \frac{1}{6}$ , para m > 6 ia cota m in m se puede disminuir en  $2 \frac{m}{6} \sum_{i=1}^{m} \frac{2a+1}{2a-1} = \frac{m}{3} \ln \left( 2 \left[ \frac{m}{6} \right] + 1 \right).$ 

La última expresión es  $> \frac{m}{2}$  si m > 12 y es > m si m > 60.

12, a. Supongamos que  $m=p_1^{\alpha_1},\dots p_k^{\alpha_k}$  es la descomposicion canónica del número m. Hactendo  $p_1^{\alpha_1}=m_1,\dots,p_k^{\alpha_k}=m_k$ , y conservando las notaciones de la pregunta 10, n, se tiene

$$\sum_{\xi_1} e^{2\pi i \cdot \frac{\xi_1}{m_1}} \cdots \sum_{\xi_k} e^{2\pi i \cdot \frac{\xi_k}{m_k}} = \sum_{\xi} e^{2\pi i \cdot \frac{\xi}{m}}.$$

Pero, al  $\alpha_d = 1$ , se obtiene

$$\sum_{\substack{a \in \mathbb{Z}_d \\ b \in \mathbb{Z}_d}} \frac{3_a}{m_a} = \sum_{\substack{a \in \mathbb{Z}_d \\ a \in \mathbb{Z}_d}} \frac{3_{ab}}{m_a} - 1 \Longrightarrow -1.$$

Si  $\alpha_a > 1$ , haciendo  $m_a = p_a m_A^2$ , se obtiene

 $0 < \alpha \leq \frac{m}{2}$ 

$$\sum_{\xi_{\theta}} e^{2\pi i \frac{\xi_{\theta}}{m_{\theta}}} = \sum_{x_{\theta}} e^{2\pi i \frac{x_{\theta}}{m_{\theta}}} - \sum_{u=0}^{m_{\theta}'-1} e^{2\pi i \frac{u}{m_{\theta}'}} = 0,$$

b. Sea m entero, m>1. Se tiene  $\sum_{x=0}^{m-1} e^{\frac{2\pi i}{m}} = 0$ . La suma de los términos del primer miembro de esta igualdad que cumplen la condición (x,m)=d, es igual a  $\mu\left(\frac{m}{d}\right)$ , en virtud del teorema de la pregunta a,

c. Obtenemos

$$\sum_{\underline{k}} e^{2\pi i \frac{\underline{k}}{m}} = \sum_{\underline{d} \setminus \underline{m}} \mu(\underline{d}) S_{\underline{d}},$$

donde, haciendo m = mod, se tiene

$$S_d = \sum_{\nu=0}^{m_0-1} e^{2\pi i \frac{\nu}{m_0}}.$$

Esta suma es igual a 0 si d < m e igual a 1 si d = m. De aquí resulta el teorema de la pregunta a.

d. Las igualdades se deducen de la pregunta 10, b.

e. Se tiene

$$A(m_1)$$
  $A(m_k) = m^{-r} \sum_{a_1} \dots \sum_{a_k} S_{a_1}, m_1 \dots S_{a_k}, m_k$ 

donde  $a_1, \ldots, a_k$  recorren los sistemas reducidos de restos respecto de los módulos  $m_1, \ldots, m_k$ . De aqui (pregunta d) se deduce inmediatamente la primera igualdad de la pregunta. La segunda igualdad se demuestra de un modo análogo.

18, a, Se tiene

$$\sum_{n=0}^{p-1} e^{2\pi i \frac{n\pi}{p}} = \left\{ \begin{array}{l} \rho, \ \text{si } n \ \text{es multiplo de } \rho, \\ 0 \ \text{en caso contrario.} \end{array} \right.$$

b. Desarrollando el producto que corresponde a un a dado resulta

$$\sum_{d \ a} \frac{\mu(d)}{d} \sum_{x=0}^{d-1} e^{2\pi i \frac{nx}{d}}.$$

De aqui, sumando respecto de todos los  $n=0, 1, \ldots, \alpha-1$ , se obtiene la expresión conocida para  $\phi(a)$ .

14. La parle de la expresión del segundo miembro que corresponde a un valor de x que es divisor de a, es igual a 1; la parle que corresponde a un valor de x que no es divisor de a, es igual a 0. De aquí que la expresión en cuestión es igual al doble del número de divisores de a, menores que  $\sqrt{a}$ , más  $\delta$ , es decir, es igual a  $\tau$  (a).

15, a, Se Hene

$$(h_1 + h_2) P =$$

$$= h_1^p + \binom{p}{1} h_1^{p-1} h_2 + \dots + \binom{p}{p-1} h_1 h_2^{p-1} + h_2^p = h_1^p + h_2^p \pmod{p};$$

$$(h_1 + h_2 + h_3) P = (h_1 + h_2) P + h_1^p = h_1^p + h_2^p + h_2^p \pmod{p}, \text{ etc.}$$

b. Haciendo  $h_1=h_0=1,\ldots=h_n=1$ , del teorema de la pregunta a se obtiene el teorema de Fermat.

c. Sea 
$$(a, p) = 1$$
. Para ciertos enteros  $N_1, N_2, ..., N\alpha$ , se tiene  $a^{(p-1)} = 1 + N_1 p$ ,  $a^{p+(p-1)} = (1 + N_1 p)^p = 1 + N_2 p^2$ ,  $a^{p^2 \cdot (p-1)} = 1 + N_2 p^2$ , ...,  $a^{p^{2n-1}(p-1)} = 1 + N_2 p^n$ ,  $a^{q} \cdot (p\alpha) = 1 \pmod{4}$ .

Sea  $m=p_{p_1}^{\alpha_1}\ldots p_k^{\alpha_k}$  la descomposición canónica del número m. Se tiene

$$\begin{split} a^{\Phi} \stackrel{(p_1^{\alpha_1})}{=} & \equiv 1 \text{ (mod. } p_1^{\alpha_1}), \dots, a^{\Phi} \stackrel{(p_k^{\alpha_k})}{=} \text{I (mod. } p_k^{\alpha_k}), \\ a^{\Phi} \stackrel{(m)}{=} & \equiv 1 \text{ (mod. } p_k^{\alpha_k}), \dots, a^{\Phi} \stackrel{(m)}{=} & \equiv 1 \text{ (mod. } p_k^{\alpha_k}), \\ a^{\Phi} \stackrel{(m)}{=} & \equiv 1 \text{ (mod. } m). \end{split}$$

## Respuestas a las preguntas del capitulo IV

1, a. El teorema se deduce inmedialamente del teorema (de la pregunta 11, a, cap. 111. b. Sea d un divisor del número m,  $m = m_0 d$ ,  $H_d$  denota la suma de los términos que cumplen la condición (a, m) = d en la expresión para Tm de la pregunta a. Se obtiene

$$H_{d} = \sum_{a_0} \sum_{n=0}^{m-1} \dots \sum_{n=0}^{m-1} s^{2ni} \frac{a_0 f(x_1, \dots, n)}{m_0},$$

donde  $a_0$  recorre el vistema reducido de restos respecto del módulo  $m_0$ . De aqui se deduce que

$$H_d = dr \sum_{a_0} \sum_{x_0=0}^{m_0-1} \dots \sum_{w_0=0}^{m_0-1} e^{2\pi i \frac{a_0 f(x_0,\dots,w_0)}{w_0}} = m^r A(m_0).$$

c. Supongamos que m>0, (a,m)=d,  $a=a_0d$ ,  $m=m_0d$ , T es la cantidad de soluciones de la congruencia ax m b (mod. m). Se tiene

$$T_m = \sum_{m=0}^{m-1} \sum_{k=0}^{m-1} e^{2\pi i \frac{m(ax-b)}{m}} = \sum_{m=0}^{m-1} \sum_{m=0}^{m-1} e^{2\pi i \frac{ma_0}{m_0} x - 2\pi i \frac{bm}{m}} = \sum_{m=0}^{d-1} e^{-2\pi i \frac{b\alpha_0}{d}} = \begin{cases} md, & \text{si } b \text{ es multiple de } d, \\ 0 \text{ en case contrario.} \end{cases}$$

**d.** Haciendo  $(a, m) = d_1$ ,  $(b, d_1) = d_2$ , ...,  $(f, d_{r-1}) = d_r$ ,  $m = d_1 m_1$ ,  $d_1 = d_2 m_2$ , ...,  $d_{r-1} = d_r m_r$ , hallamos  $d = d_r$ ,

$$\begin{split} T_m &= \sum_{\alpha = 0}^{m-1} \sum_{s=0}^{m-1} \sum_{y=0}^{m-1} \dots \sum_{w=0}^{m-1} e^{s \frac{\alpha (\alpha x + b y + \dots + f w + g)}{m}} = \\ &= m \sum_{\alpha_1 = 0}^{d_1 - 1} \sum_{y=0}^{m-1} \dots \sum_{w=0}^{m-1} e^{s \frac{\alpha_1 (b y + \dots + f w + g)}{d_1}} = \\ &= m^{r-1} \sum_{\alpha_{n-1} = 0}^{r-1} \sum_{w=0}^{m-1} \sum_{w=0}^{2m (\alpha_{r-1} (f w + g))} e^{s \frac{\alpha_{r-1} (f w + g)}{d_{r-1}}} = m^r \sum_{\alpha_{r} = 0}^{d_{r-1} - 1} e^{s \frac{\alpha_{r} - g}{d_{r}}} \end{split}$$

 a. Apliquemos el método de inducción. Conservando las notaciones de la pregunta d, supongamos que el teorema es válido para r variables.
 Consideremos la congruencia.

$$tv + ax + \dots + fw + g = 0 \pmod{m} \tag{2}$$

Sea  $(i, m) = d_0$ . La condición para que sea posible la congruencia (2), ea  $ax + \dots + fw + g = 0 \pmod{d_0}$ . La última congruencia es posible solamente si g es múltiplo de d', donde  $d' = (a, \dots, f, d_0) = (i, a, \dots, f, m)$ , en este caso, ésta admite  $d_a^{r-1}d'$  soluciones. Por consiguiente, la congruencia (2) es posible solamente en el caso en que g es múltiplo de d'; entonces, ésta admite  $d_0^{r-1}d' \left(\frac{m}{d_0}\right)^r d_0 = m^r d'$  soluciones. Por lo tanto, el teorema también es válido para r+1 variables. Pero el teorema aubsiste para una variable. Esto significa que éste alempre es válido.

2, a. Se tiene αφ (m) = 1 (mód m), α-bαφ (m)-1 = b (mód m) b. Se tiene

1 2 ... 
$$(a-1)$$
 ab  $(-1)^{a-1}$   $\frac{(p-1) \dots (p-a+1)}{1 \cdot 2 \dots a} =$   
=  $b \cdot 1 \cdot 2 \dots (1-a)$  (mód.  $p$ ),

de donde, dividiendo término a término por  $1 \cdot 2 \dots (a-1)$ , se obtiene el teorema ( $\pi d_1$ cado.

c. a) Evidentemente, es suficiente limitarnos al caso (2, b) = 1. Eligiendo el signo de un modo adecuado, se tiene  $b \pm m \approx 0 \pmod{4}$ . Sea  $2^{6}$  la máxima potencia de 2 que divide a  $b \pm m$ . Si  $\delta > k$ , se tiene

$$x = \frac{b \pm m}{2b} \pmod{m}$$

Si 8 < k, se tiene

$$2^{h-\delta}x = \frac{b \pm m}{2^{\delta}} \text{ (mod. } m).$$

Con esta congruencia repetimos una operación análoga, etc.

β) Suponemos que (3, b) = 1. Eligiendo el signo de un modo adecuado, se tiene  $b \pm m \equiv 0 \pmod{3}$ . Sea  $3^6$  la máxima potencia de 3 que divide a  $b \pm m$ . Si  $\bar{0} > h$ , se tiene

$$x = \frac{b \pm m}{3^h} \pmod{m}.$$

Si & < k, se tiene

$$3^{k+6}x = \frac{b \pm m}{2^{d}} \pmod{m},$$

Con esta congruencia repetimos una operación análoga, etc.

 $\gamma$ ) Sea p un divisor primo de a. Hallemos t de la condición b+mt = 0 (mód. p). Sea  $p^0$  la máxima potencia de p que divide a (a, b+mt), y ma  $a = a_1 p^0$ . Se tiene

$$a_1 x = \frac{b + mt}{ab}$$
 (mód. m).

St  $a_1 > 1$ , repetimos una operación análoga con esta nueva congruencia, etc.

El método Indicado es cómodo en el caso en que el número a posta factores primos no muy grandes.

3. Haciendo  $f = [\tau]$ , escribimos las congruencias

$$a \cdot 0 \equiv 0 \pmod{m},$$
  
 $a \cdot 1 \equiv y_1 \pmod{m},$   
 $a \cdot t \equiv y_t \pmod{m},$   
 $a \cdot t \equiv y_t \pmod{m},$   
 $a \cdot 0 \equiv m \pmod{m},$ 

Colocando estas congruencias en orden de crecimiento de sus segundos miembros (compárese con la pregunta 4, a, cap. II) y restando término a término cada congruencia (a excepción de la última) de la que le sigue, se obtienen i+1 congruencias de la forma  $ax = u \pmod{m}$ ;

$$0 < |z| \le \tau$$
. En este caso, al menos en una congruencia será  $0 < u < \frac{m}{\tau}$ .

En efecto, u admite  $t+1 > \tau$  valores, estos valores son positivos, y su suma es igual a m.

4, a, α) Se deduce de la definición de fracción simbólica.

β) Aqui se puede hacer  $b_0 = b + mt$ , donde t se define por la condición b + mt = 0 (mód. a); entonces, satisface a la congruencia ax = b el número entero, representado por la fracción ordinaria  $\frac{b_0}{a}$ .

y) Se tiene (bo es un múltiplo de a, do es un múltiplo de c)

$$\frac{b}{a} + \frac{d}{c} = \frac{b_0}{c} + \frac{d_0}{c} = \frac{b_0c + ad_0}{ac} = \frac{bc + ad}{ac}.$$

6) Se tiene

$$\frac{b}{a} \cdot \frac{d}{c} = \frac{b_0}{a} \cdot \frac{d_0}{c} = \frac{b_0 d_0}{ac} = \frac{bd}{ac}.$$

b, α) Se tiene (las congruencias se toman respecto del módulo ρ)

$$\binom{p-1}{a} = \frac{(p-1)(p-2) \cdot \cdot (p-a)}{1 \cdot 2 \cdot \cdot a} = \frac{(-1)^a \cdot 1 \cdot 2 \cdot \cdot \cdot a}{1 \cdot 2 \cdot \cdot \cdot a} = (-1)^a.$$

La pregunta 2, b se resuelve más fácilmente así.

$$\frac{b}{a} = \frac{b(-1)^{a-1}(p-1)\dots(p-(a-1))}{12\dots(a-1)a} \pmod{p}$$

β) Se tiene

$$\frac{2^{p}-2}{p} = 1 + \frac{p-1}{1\cdot 2} + \frac{(p-1)(p-2)}{1\cdot 2\cdot 3} + \cdots + \frac{(p-1)(p-2)\dots(p-(p-2))}{1\cdot 2\dots(p-1)} \text{ (mód. } p\text{)}.$$

5, a. Entre los números s,  $s + 1, \ldots, s + n - 1$ , ningún par puede tener simultaneamente divisores comunes con d. Los productos s (s + 1) . . . (s + n - 1) pueden ser reunidos en n× clases según la cantidad de modos con que el número d pueda dividirse en a factores primos entre si, teniendo en cuenta el orden de estos últimos (pregunta 11, b, cap 11) Ses  $d = u_1u_1$  .  $u_n$  una de tales divisiones La cantidad de productos con la condición  $s=0\pmod{u_t},\ s+1=$ , s+n-1=0 (mód.  $u_n$ ) es igual a  $\frac{a}{b}$  Por lo tanto, =0 (mód u₂).

el número buscado es igual a  $n \times \frac{a}{2}$ .

b. El número indicado es igual a

$$\sum_{d > a} \mu(d) S_d; \quad S_d = \frac{n^k a}{d},$$

donde x es igual a la cantidad de divisores primos del número d. Pero, se tiene

$$\sum_{d \geq n} \mu(d) \frac{n^{N} a}{d} \Rightarrow a \left(1 - \frac{n}{\rho_{1}}\right) \left(1 - \frac{n}{\rho_{2}}\right), \dots \left(1 - \frac{n}{\rho_{h}}\right).$$

6, a. Todos los valores de x que satisfacen a la primera congruencia vienen dados por la igualdad  $x = b_i + m_i t$ , donde t es entero. Para elegir entre éstos aquellos que satisfacen también a la segunda congruencia, hay que limitarse solamente a aquellos valores de f que satisfacen a la congruencia

$$m_1 l = b_1 - b_1 \pmod{m_2}$$
.

Pero esta congruencia es resoluble cuando, y sólo cuando, b<sub>2</sub> — b<sub>1</sub> es múltiplo de d. Además, cuando ésta es resoluble, el conjunto de valores i que la satisfacen se determina por una igualdad de la forma  $t = t_0 + \frac{m_2}{d}t'$ , donde t' es entero, el conjunto de valores  $\pi$  que satisface al sistema considerado en la pregunta se determina por la igualdad

$$x = b_1 + m_1 \left( t_0 + \frac{m^2}{d} \cdot t' \right) = x_{1, 2} + m_{1, 2} t',$$

$$x_{1,2} = b_1 + m_1 t_0.$$

b. SI el sistema

$$x = b_1 \pmod{m_1}, \quad x = b_2 \pmod{m_2}$$

es resoluble, el conjunto de valores x que le satisface se expresa por una congruencia de la forma  $x = x_{i,2} \pmod{m_{1,3}}$  Si el statema

$$x = x_{1,2} \pmod{m_{1,2}}, x = b_1 \pmod{m_2}$$

es resoluble, el conjunto de valores x que le satisface se expresa por una congruencia de la forma  $x \mapsto x_{1,2,3}$  (môd  $m_{1,3,3}$ ). Si el sistema  $x \mapsto x_{1,2,3}$  (môd  $m_{1,3,3}$ ),  $x \mapsto b_4$  (môd  $m_4$ )

es resoluble, el conjunto de valores x que le satisface se expresa por una congruencia de la forma  $x = x_{1,2,3,4}$  (mód  $m_{1,2,3,4}$ ), etc

- 7, a) Al sustituir x por -x (en virtud de lo cual x' se sustituye por -x') el valor de la suma  $\left(\frac{a,b}{-}\right)$  no varia.
- β) Cuando x recorre el sistema reducido de restos respecto del móduto m, x' también recorre el sistema reducido de restos respecto del módulo m.
- γ) Haciendo x = hz (mód m), resulta

$$\left(\frac{a, bh}{m}\right) = \sum_{s} e^{2\pi i \cdot \frac{ahs + bs'}{m}} = \left(\frac{ah, b}{m}\right).$$

Se tiene

$$\left(\frac{a_{1}, 1}{m_{1}}\right) \left(\frac{a_{2}, 1}{m_{2}}\right) = \sum_{x} \sum_{y} e^{2\pi i \frac{a_{1}m_{3}x + a_{2}m_{1}y + m_{3}x' + m_{1}y'}{m_{3}m_{2}}}$$

Haciendo  $m_{x}x' + m_{4}y' = z'$ , se tiene

 $(a_1m_2x + a_2m_1y)(m_2x' + m_1y') \Rightarrow a_1m_1^2 + a_2m_1^2 \pmod{m_1m_2},$ 

$$\left(\frac{a_1, 1}{m_1}\right) \left(\frac{a_2, 1}{m_2}\right) = \left(\frac{m_1^2 a_1 + m_1^2 a_2, 1}{m_1 m_2}\right)$$

lo cual demuestra la propiedad indicada para el caso de dos lactores. La generalización para el caso de más de dos factores es trivial.

8. La congruencia

$$a_0x^n + a_1x^{n-1} + \dots + a_n = a_0(x - x_1)(x - x_2)$$
  $(x - x_n) = 0 \pmod{\rho}$ 

admite a soluciones. Su grado es inferior a a. Por consiguiente, todos sus coeficientes son múltiplos de p, lo cual se expresa mediante las congruencias indicadas en la pregunta

9, a. Si p > 3, para cada x tomado de la sucesión 2, 3, ..., p - 2, hallamos en esta sucesión un número correspondiente x', distinto del mismo x, que cumple la condición  $xx' = 1 \pmod{p}$ , en efecto, si fuese x = x' resultaría que  $(x - 1)(x + 1) = 0 \pmod{p}$ ; x = 1 o x = p - 1. Por consiguiente,

 $2 \cdot 3 \cdot \dots (p-2) = 1 \pmod{p}; \quad 1 \cdot 2 \cdot (p-1) = -1 \pmod{p}.$ 

b. Sea P > 2. Suponiendo que P posee un divisor u que cumple la condición 1 < u < P, se tendria que  $1 \cdot 2 \cdot ... \cdot (P-1) + 1 = 1 \pmod{u}$ .

a. Hallamos un número h que cumpla la condición a<sub>0</sub>h=1 (mód. m).
 La congruencia dada equivale a la que sigue:

$$x^{n} + a_{1}hx^{n-1} + \dots + a_{n}h = 0 \pmod{m}$$
.

b. Sea Q(x) el cociente y R(x) el residuo de la división de  $x^p - x$  por f(x). Todos los coelicientes de Q(x) y R(x) son enteros. Q(x) es de grado p - n, R(x) es de grado inferior a n,

$$xP - x = f(x) Q(x) + R(x).$$

Supongamos que la congruencia  $f(x) = 0 \pmod{p}$  posee n soluciones. Estas mismas soluciones son también soluciones de la congruencia  $R(x) = 0 \pmod{p}$ . Por lo tanto, todos los coeficientes de R(x) son múltiplos de p.

Reciprocamente, supongamos que todos los coeficientes de R (x) son múltiplos de p. Entonces f (x) Q (x) es múltiplo de p para los mismos valores de x que  $x^p - x$ ; por lo tanto, la suma de los números de soluciones de las congruencias

$$f(x) = 0 \pmod{p}, \quad Q(x) = 0 \pmod{p}$$

no es menor que p. Supongamos que la primera admite  $\alpha$  soluciones y la segunda  $\beta$  soluciones. De

$$\alpha < n$$
,  $\beta ,  $p < \alpha + \beta$$ 

deductions que  $\alpha = n$ ,  $\beta = p - n$ .

e. Elevando término a término la congruencia dada a la potencia  $\frac{p-1}{n}$ , nos convencemos de que la condición indicada es necesaria Supongamos que se cumple esta condición; de

$$x^{p} - x = x \left( x^{p-1} - A^{\frac{p-1}{n}} + A^{\frac{p-1}{n}} - 1 \right)$$

se deduce que el residuo de la división de  $x^p-x$  por  $x^n-A$  es igual  $\left(A^{\frac{p-1}{n}}-1\right)_{x_1}$  donde  $A^{\frac{p-1}{n}}-1$  es múltiplo de p.

11. De  $x_0^n = A$  (mód. m),  $y^n = 1$  (mód. m) se deduce que  $(x_0y)^n = \pi A$ (mód. m); ahora bien, los productos  $x_0y$  que corresponden a valores de y incongruentes (respecto del módulo m), son incongruentes De  $x_0^n = A$  (mód. m),  $x^n = A$  (mód. m) se deduce que  $x^n = x_0^n$  (mód. m) y determinando y de la condiction  $x = yx_0$  (mód. m), se tiene

$$y^n = 1 \pmod{m}$$
.

## Respuestas a las preguntas del capitulo V

- 1. La congruencia indicada es equivalente a la siguiente  $(2ax + b)^3 = b^3 4ac \pmod{m}$  Para cada solución  $z = z_0 \pmod{m}$  de la congruencia  $z^3 = b^3 4ac \pmod{m}$  hallamos de  $2ax + b = z_0 \pmod{m}$  una solución correspondiente de la congruencia indicada
- 2, a. Si  $\left(\frac{a}{p}\right) = 1$ , so tiene  $a^{2m+1} = 1 \pmod{p}$ ,  $(a^{m+1})^3 = a \pmod{p}$ .  $x = \pm a^{m+1} \pmod{p}$ .
- b. Si  $\left(\frac{a}{p}\right) = 1$ , so tione  $a^{4m+2} = 1$  (mod. p),  $a^{2m+1} = \pm 1$  (mod. p),  $a^{2m+2} = \pm a$  (mod. p).

Como  $\binom{2}{p} = -1$ , también se tiene  $2^{4m+2} = -1$  (mód. p). Por lo tanto, para un s que toma uno de los valores 0; 1, resulta  $g^{2m+2} \cdot 2^{(4m+2) \cdot 2} = g \cdot (mód. p)$ .

c. Sea  $p = 2^h h + 1$ , donde k > 3 y h as impar,  $\left(\frac{a}{p}\right) = 1$  Se there  $a^{2^{h-1}h} \equiv 1 \pmod{p}$ ,  $a^{2^{h-2}h} \equiv \pm 1 \pmod{p}$ ,

 $N^{2^{k-1}h} = -1 \; (\bmod, \; p)$ 

Por consigniente, para cierto entero no negativo  $s_2$ , se obtiene  $a^{2^{k-b}h}N^{a_22^{k-1}} \equiv 1 \pmod{p} \quad a^{2^{k-b}h}N^{a_22^{k-2}} \equiv \pm 1 \pmod{p};$ 

de aquí, para cierto entero negativo sa, se obtiene

 $a^{2^{k-4}h}N^{a_32^{k-2}} \equiv 1 \pmod{p}, \quad a^{2^{k-4}h}N^{a_32^{k-3}} \equiv \pm 1 \pmod{p},$ 

etc.; finalmente, se obtiene

$$a^{h}N^{k_0}k \equiv 1 \pmod{p}, \quad x \equiv \pm a^{\frac{h+1}{2}}N^{s_k} \pmod{p}$$

d. Se Hene

$$1 \cdot 2 \dots 2m (p-2m) \dots (p-2) (p-1) + 1 = 0 \pmod{p},$$

$$(1 \cdot 2 \dots 2m)^{n} + 1 = 0 \pmod{p}.$$

3. a. Las condiciones de resolubilidad de las congruencias (1) y (2) se deducen trivialmente (f. § 2 y k. § 2). La congruencia (3) es resoluble cuando, y sólo cuando,  $\left(\frac{-3}{p}\right) = 1$ . Pero  $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$  y

 $\left(\frac{p}{3}\right) = \left\{\begin{array}{c} 1, \text{ si } p \text{ es de la forma } 6m+1, \\ -1, \text{ si } p \text{ es de la forma } 6m+5. \end{array}\right.$ b. Cualesquiera que sean los primos distintos  $p_1, p_2, \ldots, p_k$ de la forma 4m + 1, el divisor primo minimo p del número  $(2p_1p_2 \dots p_k)^2 + 1$  es distinto de  $p_1, p_2, \dots, p_k$  y, como  $(2p_1p_2...p_n)^3+1=0$  (mod. p), es de la forma 4m + 1 c. Cualesquiera que sean los primos distintos  $p_1, p_2, \ldots, p_k$ de la forma 6m + 1, el divisor primo mínimo p del número  $(2p_1p_2...p_k)^3 + 3$  es distinto de  $p_1, p_2, ..., p_k$  y, como  $(2p_1p_2...p_k)^3$  $p_{h})^{2}+3\equiv 0 \pmod{p}$ , es de la forma 6m+1.

4. En el primer conjunto hay números que son congruentes con 1.1, 2.2, ...,  $\frac{p-1}{2}$   $\frac{p-1}{2}$ , o sea, con todos los restos cuadráticos del sistema completo, según la condición, un número que pertenece al segundo conjunto es un no-resto cuadrático. Pero al segundo conjunto pertenecen todos los productos de este no-resto por todos los restos, es decir, pertenecen todos los no-restos cuadráticos.

5. a. Supongamos que en el sistema de numeración de base p  $a = a_{n-1}p^{n-1} + ... + a_1p + a_0$ 

y que la solución buscada (el resto mínimo no negativo) es

 $x = x_{\alpha-1}p^{\alpha-1} + \ldots + x_1p + x_0.$ (1) Formemos la tabla:

ai	***	$a_{4}$	an	a <sub>2</sub>	a <sub>1</sub>	a0
2x <sub>0</sub> x <sub>α-1</sub>		2x <sub>0</sub> x <sub>4</sub>	2x <sub>0</sub> k <sub>3</sub>	2x0x2	$2x_0x_1$	d
2x1x0-1	* 1 *	$2x_1x_3$	2x1x2	x)		
2x2xa-3		κį				

donde en la columna bajo  $a_a$  liguran los números cuya suma engendra el coeficiente de  $p^a$  en el desarrollo del cuadrado del segundo miembro (i) según las potencias de p. Hallamos  $x_0$  de la condición

$$x_0^2 = a_0 \pmod{p}$$
.

Haciendo  $\frac{x_0^2-a_0}{\rho}=\rho_1$ , obtenemos  $x_1$  de la condición

$$\rho_1 + 2x_0x_1 = a_1 \pmod{\rho}$$
.

Haciendo  $\frac{p_1+2x_0x_1-a_1}{p}=p_3$ , obtenemos  $x_3$  de la condición

$$p_1 + 2x_0x_2 + x^* = a_2 \pmod{p}$$

etc. Como  $(x_0,\ p)=1$ , para el número  $x_0$  dado, los números  $x_1,\ x_3,\dots$  ...,  $x_{m-1}$  se determinan univocamente.

b. Aqui

$$a = a_{\alpha-1}2^{\alpha-1} + \dots + a_32^{\alpha-1} + a_22^{\alpha} + a_42 + a_0,$$

$$x = x_{\alpha-1}2^{\alpha-1} + \dots + x_32^{\alpha} + x_42^{\alpha} + x_42 + x_{00}$$

y se tiene la tabla siguiente:

$a_{\alpha-i}$		$a_4$	ag	a <sub>3</sub>	$a_1$	a
X0E@-1		x <sub>0</sub> x <sub>3</sub>	K <sub>0</sub> E <sub>2</sub>	ZoX;		x)
x <sub>1</sub> x <sub>0=3</sub>	444	$x_ix_2$		z]		
x <sub>b</sub> x <sub>m-4</sub>		23				

Consideremos solamente el caso  $\alpha > 3$  Como (a, 2) = 1, tiene que ser necesariamente  $a_0 = 1$ . Por lo tanto,  $x_0 = 1$ . Luego tiene que ser necesariamente  $a_1 = 0$  y, como  $x_0x_1 + x_1^2 = x_1 + x_1^2 = 0$  (mód. 2), tiene que ser necesariamente  $a_2 = 0$  Para  $x_1$  son posibles dos valores: 0 y 1 Los números  $x_2$ ,  $x_3$ , ...,  $x_{\alpha-1}$  se determinan univocamente, y para  $x_{\alpha-1}$  son posibles dos valores: 0 y 1 Por totanto, si  $\alpha > 3$  tiene que ser necesariamente  $\alpha = 1$  (mód. 8), y entonces la congruencia indicada admite 4 soluciones

6. Evidentemente,  $P ext{ y } Q$  son enteros,  $y ext{ Q}$  es congruente respecto del módulo p con el número que se obtiene al sustituir a por  $x^2$ , para lo cual es suficiente sustituir  $\sqrt{a}$  por x. Por lo tanto,  $Q = 2^{a-1}x^{a-1}$  (mód. p); por consiguiente, (Q, p) = 1 y Q' verdaderamente se puede determinar de la congruencia  $QQ' \Rightarrow 1$  (mód.  $p^3$ ). Se tiene

$$P^{\underline{a}} - aQ^{\underline{a}} = (z + \sqrt{a})^{\alpha} (z - \sqrt{\alpha})^{\alpha} = (z^{\underline{a}} - a)^{\alpha} = 0 \text{ (mod. } p^{\alpha}),$$

de donde

$$(PQ')^3 = a(QQ')^3 = a \pmod{p^2}.$$

7. Sea  $m=2^{\alpha}\rho_1^{\alpha_1}\dots,\ \rho_k^{\alpha_k}$  is descomposición canónics del número m. Entonces m se express de  $2^k$  maneras en la forma  $m=2^{\alpha}ab$ , donde (a,b)=1. Supongamos que  $\alpha=0$ . De (x-1)(x+1)=0 (mód m) se deduce

Supongamos que  $\alpha = 0$ . De  $(x - 1)(x + 1) = 0 \pmod{m}$  se que para ciertos  $\alpha y b$ .

$$x = 1 \pmod{a}$$
;  $x = -1 \pmod{b}$ .

Resolviendo este sistema se obtiene  $x=x_0\pmod m$ . Por lo tanto, la congruencia indicada tiene  $2^h$  soluciones.

Supongamos que  $\alpha = 1$ . Para ciertos a y b

$$x = 1 \pmod{2a}; \quad x = -1 \pmod{2b}.$$

Resolviendo este sistema se obtiene  $x=x_0\pmod m$ . Por lo tanto, la congruencia indicada tiene  $2^h$  soluciones.

Supongamos que a - 2. Para ciertos a v 5

$$x = 1 \pmod{2a}; \quad x = -1 \pmod{2b}.$$

Resolviendo este sistema se obtiene  $x = x_0 \pmod{\frac{m}{2}}$ . Por lo tanto, la congruencia indicada tiene  $2^{k+1}$  soluciones.

Supongamos que  $\alpha > 3$ . Para ciertos  $\alpha$  y b tiene que verificarse uno de los sistemas

$$x = 1 \pmod{2a};$$
  $x = -1 \pmod{2^{\alpha-1}b};$   $x = -1 \pmod{2^{\alpha-1}b};$   $x = -1 \pmod{2b}.$ 

Resolviendo uno de estos sistemas se obtiene  $x = x_0 \pmod{\frac{m}{2}}$ . Por lo tanto, is congruencia indicada tiene  $2^{n+2}$  soluciones.

8. a. Determinando x de la congruencia  $xx' = 1 \pmod{p}$ , se tiene

$$\sum_{x=1}^{p-1} \left( \frac{x(x+k)}{p} \right) = \sum_{x=1}^{p-1} \frac{(xx'(xx'+kx'))}{p} = \sum_{x=1}^{p-1} \left( \frac{1+kx'}{p} \right).$$

Evidentemente, 1+kx' recorre todos los restos del assterna completo, a excepción de 1. De aquí se deduce el teorema indicado.

b. La igualdad en cuestión se deduce de la igualdad

$$\mathbf{T} = \frac{1}{4} \sum_{x=1}^{p-2} \left( 1 + \varepsilon \left( \frac{x}{p} \right) \right) \left( 1 + \eta \left( \frac{x+1}{p} \right) \right) =$$

$$= \frac{1}{4} \sum_{x=1}^{p-2} \left( 1 + \varepsilon \left( \frac{x}{p} \right) + \eta \left( \frac{x+1}{p} \right) + \varepsilon \eta \left( \frac{x(x+1)}{p} \right) \right).$$

e. Supongamos que  $\delta$  denota la cantidad de valores de y que son iguales a cero (por consiguiente,  $\delta = 0$  ó  $\delta = 1$ ). Se tiene

$$S^2 < X \sum_{y_1} \sum_{y} S_{y_1, y}; S_{y_1, y} = \sum_{n=0}^{p-1} \left( \frac{(xy+h)(xy_1+h)}{p} \right).$$

Ahora hallamos que

 $S_{w_{i+1}u}=p$ , at  $y_1=y=0$ ;

 $S_{y_{n+1}} = 0$ , si solamente uno de los números  $y_1$  e y es igual a cero;

$$S_{y_1,y}=p-1=p-\left(\frac{y_1y}{p}\right), \quad \text{if } y_1=y>0;$$

$$S_{y_1, y} = \left(\frac{y_1 y}{\rho}\right)$$
 en los demás casos.

Por lo tanto,

$$S^3 \leqslant X \left( pb + p \left( Y - b \right) - \left( \sum_{n > 0} \left( \frac{y}{p} \right) \right)^2 \right) \leqslant XYp.$$

d. a) Se trene

$$S = \sum_{r=0}^{p-1} \sum_{r=0}^{Q-1} \sum_{r=0}^{Q-1} \left( \frac{(x+z_1)(x+z)}{p} \right) .$$

Para  $z_1 = z$ , la sumación respecto de x da p-1. Para  $z_1$  distinto de z, la sumación respecto de x (pregunta a) da -1. Por lo tanto,  $S = pQ - Q^2$ .

β) Según el teorema de la pregunta α), se tiene

$$T(Q^{0.6+0.6h})^2 \le S \le pQ$$
;  $T \le pQ^{-1}$ .

γ) SI  $p \le 6$ , el teorema es trivial. Si p > 5, aplicamos el teorema de la pregunta  $\alpha$ ). Suponiendo que en la sucesión indicada en la pregunta

no hay no-restos cuadráticos, llegamos a la conclusión que  $S_x = Q$  para x = M,  $M+1, \ldots, M+Q$ . Por lo tanto  $(Q^n + 2Q + 2Q + 1)$  no son iguales a p, puesto que son compuestos), hallamos

$$(Q+1) Q^0 \le (p-Q) Q$$
,  $Q^0 + 2Q < p$ ,  $(Q+1)^0 < p$ .

lo cual es imposible.

9. a. Si m se expresa en la forma (I), la solución

$$z = z_0 \pmod{m}$$
 (5)

de la congruencia  $x = xy \pmod{m}$  también es solución de la congruencia (2) Diremos que la expresión indicada está ligada con la solución (5) de la congruencia (2)

Con cada solución (5) de la congruencia (2) está ligada no menos de una expresión (1). En efecto, tomando  $\tau = \sqrt{m}$ , se tiene

$$\frac{z_0}{m} = \frac{P}{Q} + \frac{\theta}{Q\sqrt{m}}; \quad (P, Q) = 1, \quad 0 < Q < \sqrt[n]{m}, \quad |\theta| < 1.$$

Por lo tanto,  $z_0Q = mP + r$ , donde  $|r| < \sqrt{m}$ . Luego, de (2) se deduce que  $|r|^2 + Q^2 \equiv 0 \pmod{m}$ . De squí y de  $0 < |r|^2 + Q^2 < 2m$  se obtiene

$$m = |r|^2 + Q^2$$
. (6)

Ahora bien, (|r|, Q) = 1, puesto que

$$1 = \frac{r^2 + Q^2}{m} = \frac{(z_0 Q - mP) z_0 Q - rmP + Q^2}{m} = -rP \pmod{Q}.$$

Si |r| = r,  $r = z_0 Q$  (mód. m), la expresión (6) está ligada con la solución (5) Si |r| = -r, como  $z_0^2 Q$  em  $z_0 r$  (mód m),  $Q = z_0 |r|$  (mód m), la expresión  $m = Q^2 + |r|^2$  está ligada con la solución (5). Con cada solución (6) está ligada no más de una expresión (1) En efecto, si dos expresiones del número m en la forma (1),  $m = x^2 + y^3$  y  $m = x_1^2 + y_1^2$ , están ligadas con una solución (5), entonces, de  $x = z_0 y$  (mód. m),  $x_1 = z_0 y$  (mód. m) se deduce que  $xy_1 = x_1 y$  (mód. m). Por lo tanto,  $xy_1 = x_1 y$ , y como  $(x, y) = (x_1, y_1) = 1$ , resulta que  $x = x_1$ ,  $y = y_1$ .

b. Si p se expresa en la forma (3), la solución

$$z = z_0 \pmod{\rho}$$
 (7)

de la congruencia  $x = xy \pmod{p}$  también es solución de la congruencia (4). Diremos que la expresión indicada está ligada con la solución (7) de la congruencia (4).

Conociendo la solución (7) de la congruencia (4), hallamos no menos de una expresión (3). En efecto, tomado  $\tau = \sqrt{\rho}$ , se tiene

$$\frac{z_0}{\rho} = \frac{P}{Q} + \frac{\theta}{Q \sqrt{\rho}}, \quad (P, Q) = 1, \quad 0 < Q \le \sqrt{\rho}, \quad |\theta| < 1.$$

Por lo tanto,  $z_0Q = r \pmod p$ , donde  $|r| < \sqrt{p}$ . Luego, de (4) se deduce que  $|r|^2 + aQ^2 = 0 \pmod p$ . De aquí y de  $0 < |r|^2 + aQ^2 < (i + a) p$  se deduce que, si a = 2, tiene que ser  $|r|^2 + 2Q^2 = p$  6  $|r|^3 + 2Q^2 = 2p$ . En el último caso |r| es par,  $|r| = 2r_1$ ,  $p = Q^2 + 2r_1^2$ . Si a = 3, tiene que ser  $|r|^2 + 3Q^2 = p$ , 6  $|r|^3 + 3Q^2 = 2p$ , 6  $|r|^3 + 3Q^2 = 3p$  El segundo caso es imposible, pues, respecto del módulo 4 el primer miembro es congruente con 0, mientras que el segundo miembro es congruente con 2. En el tercer caso, |r| es múltiplo de 3,  $|r| = 3r_1$ ,  $p = Q^3 + 3r_1^3$ . Suponiendo que dos expresiones del número p en la forma (3),  $p = x^3 + ay^3$  y  $p = x_1^3 + ay_1^3$ , están ligadas con una misma solución de la congruencia (4), hallamos que  $x = x_1$ ,  $y = y_1$ . Suponiendo que estas expresiones están ligadas con soluciones distintas de la congruencia (4), hallamos que  $x = x_1$ ,  $y = y_1$ . Suponiendo que estas expresiones están ligadas con soluciones distintas de la congruencia (4), hallamos que  $x = x_2$  (mód p),  $x_1 = -xy_1$  (mód p),

$$0 < (xy_1 + x_1y)^2 < (x^3 + y^2)(x_1^3 + y_1^3) < p^3$$

c,  $\alpha$ ) Los términos de la suma S(k) con  $x=x_1$  y  $x=-x_1$  son iguales  $\beta$ ) Se tiene

de donde  $xy_1 + x_1y = 0$  (mód. p), lo cual es imposible, puesto que

$$S(kl^3) = \sum_{n=0}^{p-1} \left( \frac{kl \left( x^2 l^3 + kl^2 \right)}{p} \right) = \left( \frac{t}{p} \right) S(k).$$

γ) Haclendo  $\rho = 1 = 2\rho_1$ , se tiene

$$p_{1}(S(r))^{2} + p_{1}(S(n))^{2} = \sum_{t=1}^{p_{1}} (S(rt^{2}))^{2} + \sum_{t=1}^{p_{1}} (S(nt^{2}))^{2} =$$

$$= \sum_{k=0}^{p-1} S(k)^{2} = \sum_{x=1}^{p-1} \sum_{y=1}^{p-1} \sum_{k=0}^{p-1} \left( \frac{ny(x^{2}+k)(y^{2}+k)}{\rho} \right).$$

St y no es igual a x o a p-x, el resultado de la sumación respecto de k es igual a  $-\left(\frac{xy}{\rho}\right)$ ; si y=x o y=p-x éste es igual a  $(p-1)\times\left(\frac{xy}{\rho}\right)$ . Por lo tanto,  $\rho_1\left(S\left(r\right)\right)^2+\rho_1\left(S\left(n\right)\right)^2=4\rho\rho_1,\ \rho=\left(\frac{1}{2}S\left(r\right)\right)^2+\left(\frac{1}{2}S\left(n\right)\right)^2$ 

10. a. Se (fene

$$X^2 - DY^3 = (x_1 + y_1 \ V \hat{D}) (x_2 \pm y_2 \ V \overline{D}) (x_1 - y_1 \ V \overline{D}) (x_2 \pm y_2 \ V \overline{D}) = h^3.$$

b. Tomando cualquier  $\tau_1$  que cumpla la condición  $\tau_1 > 1$ , hallamos unos enteros  $x_1, y_1$  que cumplen la condición  $y_1 \sqrt{D} - x_1 > \frac{1}{\tau_1}$ ,  $0 \le y_1 \le \tau_1$ , de donde, multiplicando término a término por  $y_1 \sqrt{D} + x_1 < 2y_1 \sqrt{D} + 1$ , obtenemos  $|x_1^0 - Dy_1^0| < 2\sqrt{D} + 1$ . Tomando  $\tau_2 > \tau_1$  de modo que sea  $|y_1 \sqrt{D} - x_1| > \frac{1}{\tau_2}$ , hallamos unos nuevos enteros  $x_2, y_2$  que cumplen la condición  $|x_1^0 - Dy_1^0| < 2\sqrt{D} + 1$ , etc. De aquí se deduce que en el intervalo  $-2\sqrt{D} - 1 < k < 2\sqrt{D} + 1$  existe un entero k, distinto de cero, tal que entre los pares  $x_1, y_1, x_2, y_2, \dots$  hay un conjunto infinito de pares  $x_1, y_2$  que cumplen la condición  $x^2 - Dy^2 = k$ ; entre estos últimos siempre habrá dos pares  $\xi_1, \eta_1$  y  $\xi_2, \eta_2$  que satisfacen a la condición  $\xi_1 = \xi_2$  (mód. |k|),  $\eta_1 = x_1$   $\eta_1$  (mód. |k|). Determinando los enteros  $\xi_0, \eta_0$  mediante la igualdad

$$\begin{aligned} \xi_0 + \eta_0 \sqrt[n]{D} = (\xi_1 + \eta_1 \sqrt{D}) & (\xi_2 - \eta_1 \sqrt{D}), \text{ se time (pregunta a)} \\ \xi_0^2 - D\eta_0^2 = \int_{\mathbb{R}} k_1^2 \cdot \xi_0 = \xi_1^2 - D\eta_1^2 = 0 & (\text{mod. } |k|), \\ \eta_0 = -\xi_1 \eta_1 + \xi_1 \eta_1 = 0 & (\text{mod. } |k|). \end{aligned}$$

Por lo tanto,  $\xi_0 = \xi |k|$ ,  $\eta_0 = \eta |k|$ , donde  $\xi$  y  $\eta$  son enteros y  $\xi^2 = D\eta^2 = 1$ ,

c. Los números x, y que se determinan por la igualdad (2) satisfacen (pregunta a) a la ecuación (1).

Supontendo que existe un par de enteros positivos x, y que satisfacen a la ecuación (1), pero distinto de los pares que se determinan por la igualdad (2), para cierto r=1, 2, ... tendremos

$$(x_0 + y_0 \sqrt{D})^r < x + y \sqrt{D} < (x_0 + y_0 \sqrt{D})^{r+1}.$$

De aquí, dividiendo término a término por  $(x_0 + y_0 \sqrt{D})^r$ , obtenemos

$$1 < X + Y \sqrt{D} < x_0 + y_0 \sqrt{D}, \tag{3}$$

donde (pregunta a) X e Y son enteros que se determinan por la Igualdad

$$X + Y\sqrt{D} = \frac{x + y\sqrt{D}}{(x_0 + y_0\sqrt{D})^r} = (x + y\sqrt{D})(x_0 + y_0\sqrt{D})^r$$

y satisfacen a la ecuación

$$X^2 - DY^2 = 1.$$
 (4)

Pero de (4) se deducen las designaldades  $0 < X - Y \sqrt{D} < 1$ , las cuales, junto con la primera designaldad (3), muestran que  $X \in Y$  son positivos. Por lo tanto, la segunda designaldad (3) contradice a la difinición de los números  $x_0$ ,  $y_0$ .

$$|U_{a,p}|^2 = U_{a,p} \overline{U}_{a,p} = \sum_{t=1}^{p-1} \sum_{s=1}^{p-1} \left(\frac{t}{p}\right) e^{2\pi i \frac{ax(t-t)}{p}}.$$

Para t=1 la sumación respecto de x da p-1; para t>1 resulta  $-\left(\frac{t}{p}\right)$ . Por lo tanto

$$|U_{d_{1,p}}|^{1}=p-1-\sum_{l=2}^{p-1}\left(\frac{l}{p}\right)=p,\ |U_{d_{1,p}}|=\sqrt{p}.$$

.....

$$\|U_{a,\,p}\|^2 = U_{a,\,p}\overline{U}_{a,\,p} = \sum_{l=0}^{p-1} \sum_{s=0}^{p-1} \left(\frac{s+t}{\rho}\right) \left(\frac{s}{p}\right) e^{\frac{s}{2}\pi i \frac{st}{p}}.$$

Para t=0 la sumación respecto de x da p-1; para t>0 resulta  $-\frac{2\pi i}{\sigma}\frac{\sigma t}{p}$ . Por lo tanto

$$|U_{a,p}|^2 = p - 1 - \sum_{i=1}^{p-1} e^{\frac{2\pi i}{p}} = p, \quad |U_{6,p}| = \sqrt{p}.$$

β) Si (a, p) = p el teorema es evidente. Si (a, p) = 1 éste se deduce de

$$U_{a, p} = \left(\frac{a}{p}\right) \sum_{n=1}^{p-1} \left(\frac{ax}{p}\right) e^{2\pi i \frac{ax}{p}} = \left(\frac{a}{p}\right) U_{1, p}.$$

 b, α) Supongamos que r recorre los restos cuadráticos, y n los no-restos cuadráticos, comprendidos en el sistema completo de restos.
 Se tiene

$$S_{a_1,p}=1+2\sum_{r}e^{2\pi i\frac{4r}{p}}.$$

Restando de aqui término a término

$$0=i+\sum_{\alpha}e^{\frac{2\pi i}{\beta}\frac{\alpha p}{\beta}}+\sum_{\alpha}e^{\frac{2\pi i}{\beta}\frac{\alpha m}{\beta}}$$

se obtjene la igualded indicada,

B) Se tiene

$$[S_{a,m}]^2 = \sum_{t=0}^{m-1} \sum_{r=0}^{m-1} e^{2\pi i \frac{a(t^2+2tx)}{m}}.$$

Para un t dado la sumación respecto de x da  $me^{-2\pi i \frac{-at^2}{m}}$  ó 0, según que sea divisible 2t por m o no, St m es t impar, se t tiene

$$|S_{n,m}|^2 = me^{2\pi i \frac{\alpha - 0^2}{m}} = m.$$

Si m es par, m=2m1, se tiene

$$|S_{\alpha,m}|^2 = m \left(e^{2\pi i \frac{\alpha \cdot 00}{m}} + e^{2\pi i \frac{\alpha \cdot m_1^2}{m}}\right)$$

Aqui el segundo miembro es igual a cero si  $m_1$  es impar y es igual a 2m si  $m_2$  es par.

y) Para cualquier entero b, se tiene

$$\{S_{A,m}\} = \Big|\sum_{m=1}^{m-1} e^{2\pi i \frac{Ax^{n}+2Abx}{m}}\Big|\,,$$

de donde, eligiendo b de la condición  $2Ab \approx a$  (mód. m), se obtiene (pregunta  $\beta$ ) el resultado indicado.

12, a, a) Se tiene

$$m\sum_{z}^{z}\Phi\left(z\right)=\sum_{z}\sum_{s=M}^{M+Q-1}\sum_{\alpha=0}^{m-1}\Phi\left(z\right)e^{\frac{2\pi i}{2\pi i}\frac{\sigma\left(z-s\right)}{m}}.$$

Le parte de la suma del segundo miembro que corresponde a  $a \approx 0$ , es igual a  $Q \sum_{i=0}^{\infty} \Phi(z)$ ; la parte que corresponde a los valores restantes de a es en valor absoluto (pregunta 11, c, cap. III)

$$<\Delta \sum_{m=1}^{m-1} \Big| \sum_{k=M}^{M+Q-1} e^{2\pi i \frac{-a}{m}} \Big| < \Delta m (\ln m - b).$$

β) Es suficiente demostrar que la suma

$$T = \sum_{v} \sum_{y=0}^{l} \sum_{y_1=0}^{l} \sum_{n=0}^{m_1-1} e^{2\pi i \frac{\alpha(x-N-y+y_1)}{m}},$$

la cual es igual ai producto de m por el número de soluciones de la congruencia  $z = N - p + y_4 \pmod{m}$ , es positiva. Pero la parte de esta suma que corresponde a a = 0, es igual a

$$ZA^{0}; \quad A = I + I.$$

La parte que corresponde a un valor a>0 dado, es en valor absoluto menor que

$$\Delta_0 \min \left( h^2, \frac{1}{4 \left( \frac{a}{m} \right)^2} \right)$$

Por consiguiente, la parte que corresponde a todos los valores positivos a, es en valor absoluto menor que

$$2\Delta_0\sum_{\alpha=1}^\infty\min\left(h^2,\,\frac{m^2}{4a^4}\right)<2\Delta_0\left(\int\limits_0^\frac{m}{2h}h^2\,d\alpha+\int\limits_{\frac{m}{2h}}^\infty\frac{m^3}{4a^2}\,d\alpha\right)=2\Delta_0mh.$$

Per le tante.

$$T > Zh^3 - 2\Delta_0 mh > 0$$
.

b,  $\alpha$ ) Se deduce del teorema de la pregunta 11, a,  $\alpha$ ) y del teorema de la pregunta a.

β) La desigualdad de la pregunta α) da R-N=0  $V \widetilde{p} \ln p$ . Además, es obvio que R+N=Q.

y) Del teorema de la pregunta 11, b,  $\beta$ ) se deduce que se cumplen las condiciones del teorema de la pregunta a,  $\alpha$ ) si se hace  $m=p, \Phi(z)=1$   $A=\sqrt{p}$ , y z recorre los valores  $z=x^2, x=0, 1, \dots, p-1$  Pero entre los valores de z hay uno que es congruente respecto del módulo p con 0 y sendos pares que son congruentes respecto del módulo p con cada resto cuadrático del sistema completo. Por lo tanto,

$$\sum_{z}' \Phi(z) = 2R, \quad \sum_{z} \Phi(z) = p$$

y se obtiene

$$2R = \frac{Q}{p} \rho + \theta \sqrt{\rho} \ln \rho.$$

δ) Se deduce del teorema de la pregunta 11, b, γ) y del teorema de la pregunta a, α).

s) Del teorema de la pregunta ô) se deduce que se cumplen las condiciones del teorema de la pregunta a,  $\alpha$ ) si se hace m=p,  $\mathfrak{D}(z)=1$ ,  $\Delta=\sqrt{p}$  in p, y z recorre los valores  $z=Ax^2$ ;  $x=M_0$ ,  $M_0+1$ , ...,  $M_0++Q_0-1$ . Por lo tanto,

$$\sum_{z}'\Phi\left(z\right)=T_{1}\qquad\sum_{z}\Phi\left(z\right)=Q_{0},$$

de donde se deduce la fórmula índicada en la pregunta.

c. La parte de la suma que contiene los términos con  $\left(\frac{\alpha}{\rho}\right)=1$ , es igual a  $\rho\left(R^2+N^3\right)$ , la parte restante es igual a -2pRt'. Por lo tanto, toda la suma es igual a  $\rho\left(R-N\right)^3$ .

La parte de la suma que contiene los términos con a=0, es Igual a 0. La parte restante es en valor absoluto menor (pregunta 18, c, cap. 111),

$$\sum_{\alpha=1}^{p-1} \big| \sum_{x=M}^{M+Q-1} e^{2\pi i \frac{\alpha x}{p}} \big| \sum_{\alpha=1}^{p-1} \big| \sum_{y=M}^{M+Q-1} e^{2\pi i \frac{\alpha \alpha y}{p}} \big| < \rho^{3} (\ln p)^{3}.$$

Por consiguiente,

$$P(R-N)^{\mathfrak{g}} < p^{\mathfrak{g}} (\ln p)^{\mathfrak{g}}, \quad |R-N| < \sqrt{p} \ln p.$$

#### Respuestas a las preguntas del capitalo VI

- 1, a. Si q es un número primo impar y  $a^p = 1 \pmod{q}$ , entonces a respecto del módulo q pertenece a uno de los exponentes  $\delta = 1$ , p. Si  $\delta = 1$ , se tiene  $a = 1 \pmod{q}$ , si  $\delta = p$ , se tiene q = 1 = 2px, x es entero.
- b. SI q es un número primo impar y  $a^p + 1 = 0 \pmod{q}$ , entonces  $a^{kp} = 1 \pmod{q}$  Por lo tanto, respecto del módulo q el número a perfenece a uno de los exponentes b = 1, a, a, a, a, a, Los casos a = 1; a son imposibles. Si a = 2, se tiene  $a^3 = 1 \pmod{q}$ ,  $a + 1 = 0 \pmod{q}$ . Si a = 2a, se tiene a = 1 = 2a; a es entero.
- c. Son primos de la forma 2px+1, por ejemplo, los divisores primos del número  $2^p-1$  Sean  $p_1, p_2, \ldots, p_k$  cualesquiera k números primos de la forma 2px+1; el número  $(p_1, p_2, \ldots, p_k)^p-1$  posee un divisor primo de la forma 2px+1, distinto de  $p_1, p_2, \ldots, p_k$
- d. Si q es primo y  $2^{2^n} + 1 = 0 \pmod{q}$ , entonces  $2^{2^{n+1}} = 1 \pmod{q}$ . Por lo tanto, respecto del módulo q el número 2 pertenece al exponente  $2^{n+1}$  y, por consiguiente,  $q-1=2^{n+1}$  x; x es entero.
- 2. Evidentemente, respecto del módulo  $a^n 1$  el número a pertenece el exponente n. Por lo tanto, n es un divisor de  $\varphi(a^n 1)$ .
- \$, a. Supongamos que después de realizar la A-ésima operación se obtiene la sucesión inicial Evidentemente, la A-ésima operación es equivalente a la siguiente: en la sucesión

.1, 2, ..., 
$$n = 1, n, n, n = 1, \ldots, 2, 1, 1, \ldots$$

se toman los números que ocupan los lugares 1,  $1+2^h$ ,  $1+2\cdot 2^h$ Por lo tanto, en la sucesión inicial, en el  $1+2^h$  lugar tiene que estar el número 2 Por consiguiente, la condición indicada en la pregunta es necesaria. Pero ésta también es suficiente, puesto que al cumplirse se tienen las siguientes congruencias respecto del módulo 2n-1:

 $1 = 1, 1 + 2^h = 0, 1 + 2 \cdot 2^h = -1, \dots$ 

 $1 = 1, 1 + 2^h = 2, 1 + 2 \cdot 2^h = 3,$ 

o bien

b. La solución es análoga a la solución de la pregunta a.

4. La solución de la congruencia  $x^6$  mi l (mód.  $\rho$ ) pertenece a un exponente de la forma  $\frac{\delta}{\delta r}$ , donde  $\delta r$  es un divisor de  $\delta$ . Aqui  $\delta r$  es un

múltiplo de d cuando, y sólo cuando,  $x^{\frac{5}{d}} \equiv 1 \pmod{p}$ . Escribiendo todos los  $\hat{0}$  valores de  $\hat{0}'$  y tomando  $f \equiv 1$ , obtenemos  $S' = \sum_{d \in \hat{0}} \mu(d) S_d$ ,

donde S' es el número buscado y  $S_d = \frac{\delta}{d}$ .

5, s. Aquí (§ 3; ejemplo c, § 6) tiene que ser  $\left(\frac{\beta}{2^n+1}\right) = -1$ . Esta condición se cumple para g=3.

b. Aquil no tiene que ser  $\left(\frac{g}{2\rho+1}\right)=1$ ,  $g^3=1\pmod{2\rho+1}$ . Esta condición se cumple para los valores indicados de g.

c. Aqui no tiene que ser  $\left(\frac{g}{4p+1}\right)=1$ ,  $g^{q}=1$  (mód. 4p+1). Esta condición se cumple para g=2.

d. Aqui no tiene que ser  $\left(\frac{g}{2^n\rho+1}\right) = 1$ ,  $g^{2n} = 1 \pmod{2^{n\rho+1}}$ . Esta

condición se cumple para g=3.

6, a,  $\alpha$ ) Si n es múltiplo de  $\rho-1$ , el teorema es evidente Supongamos que n no es divisible por  $\rho-1$ . Los números 1, 2, ...,  $\rho-1$ , sin tener en cuenta el orden que siguen, son congruentes respecto del módulo  $\rho$  con los números g, 2g, ...,  $(\rho-1)g$ , donde g es una raíz primitiva respecto del módulo  $\rho$ . Por lo tanto,

 $S_n \equiv g^n S_n \pmod{p}, \quad S_n \equiv 0 \pmod{p}.$  So tiene

 $\sum_{r=1}^{p-1} \left( \frac{x(x^2+1)}{p} \right) = \sum_{r=1}^{p-1} x^{\frac{p-1}{2}} (x^2+1)^{\frac{p-1}{2}} \pmod{p},$ 

de donde (pregunta a)) se obliene el resultado indicado.

b. SI p > 2, se tiene

1.2. 
$$(p-1) \equiv g^{1+2+\cdots+p-1} \equiv g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$
.

7, a. Se tiene  $g_1^{\operatorname{ind} g_2 a} \equiv a \pmod{p}$ ,  $\operatorname{ind}_{g_1} a \operatorname{ind}_{g} g_1 \equiv \operatorname{ind}_{g} a \pmod{p-1}$ ,  $\operatorname{ind}_{g_2} a \equiv a \pmod{g} \pmod{p-1}$ ,

b. De  $\operatorname{ind}_{g,a} = s \pmod{n}$ .  $\operatorname{ind}_{g_1} a = \alpha \operatorname{ind}_{g} a \pmod{p-1}$  se deduce que  $\operatorname{ind}_{g_n} a = \alpha s = s_1 \pmod{n}$ .

8. Sea (n, p-1)=1. Hallando u de la condición  $nu = 1 \pmod{p-1}$ , obtenemos la solución  $x = a^u \pmod{p}$ ,

Supongamos que n es primo,  $\rho - 1 = n^{\alpha}t$ ,  $\alpha$  es un entero positivo,

 $(t, n) \approx 1$ . Si la congruencia es posible, se tiene  $a^{n^{\alpha-1}t} \equiv 1 \pmod{p}$ ,

si a>1, entonces, observando que  $z=g^{nm-1}$ tr (mód.  $\rho$ ), r=0, 1, ..., n-1, son todas las soluciones de la congruencia  $z^n=1$  (mód.  $\rho$ ), para cierto  $r_1=0$ , 1, ..., n-1, se tiene

$$a^{n\alpha-2}tg^{n\alpha-1}tr_1=1 \text{ (mod. p)};$$

si  $\alpha > 2$ , para cierto  $r_0 = 0, 1, ..., n - 1$ , se tiene

$$a^{n^{\alpha-3}i}g^{n^{\alpha-3}ir_1+n^{\alpha-1}ir_3} \Rightarrow 1 \pmod{p}$$

etc.; finalments, para cierto  $r_{\alpha-1}=0, 1, \ldots, n-1$ , se tiene

$$a^{i}g^{nir_1+nkir_2+} + +^{n\alpha-1}tr_{\alpha-1} = 1 \pmod{p}.$$

Hallando u y v de la condición tu - nv = -1, se obtienen n soluciones

$$x = a^{\eta} g^{ut(r_1 + nr_2 + \dots + n^{2r_1} - 1) + n^{2r_1 + 1} tr} \pmod{p};$$
 $r = 0, 1, \dots, n-1.$ 

Supongamos que el número primo  $n_1$  es un divisor de (n, p-1),  $n = n_1 n_2$ ,  $n_2 > 1$ . Para cada solución de la congruencia  $y^{n_1} = a$   $m = a \pmod{p}$  buscamos una solución correspondiente de la congruencia  $x^{n_2} = y \pmod{p}$ 

**8**, a. Del modo indicado se obtienen  $cc_0c_1$ ...  $c_k = \varphi$  (m) caracteres Supongamos que para dos caracteres  $\chi_1$  (a) y  $\chi_2$  (a) son distintos entre ai los valores R' y R'' de alguna de las raices R,  $R_0$ ,  $R_1$ , ...,  $R_k$ ; para el número  $a_1$ , cuyos índices son todos iguales a 0, a excepción de uno, correspondiente a los valores indicados R' y R'', e igual a 1, se tiene

$$\chi_1(a_i) = R', \ \chi_1(a_i) = R''.$$

b, a) Se tjene  $\chi(1) = R^0$  ..  $R_A^0 = 1$ .

β) Sean γ', ..., γ', γ', ..., γ' los sistemas de índices de los números as y as; entonces y' + y', ... y's + y's es el sistema de indices del número a<sub>t</sub>a<sub>2</sub> (c, § 7).

y) Si  $a_t \equiv a_2$  (mód. m), los índices de los números  $a_t$  y  $a_2$  son congruen-

tes entre si respecto de los módulos  $c_1, \ldots, c_k$ 

e. La propiedad indicada se deduce de

$$\sum_{\alpha=0}^{m-1} \chi(\alpha) = \sum_{\gamma=0}^{c-1} R^{\gamma} \cdot \sum_{\gamma_{k}=0}^{c_{k}-1} R_{k}^{\gamma_{k}}.$$

d. La propledad indicada se deduce de

$$\sum_{\chi}\chi\left(\alpha\right)=\sum_{R}R^{\gamma}\cdots\sum_{R_{h}}R_{h}^{\gamma_{h}}.$$

e. Supongamos que  $\psi(a_1)$  no es igual a 0, de la igualdad  $\psi(a_1)$  =  $= \psi(a_i) \psi(1)$  se deduce que  $\psi(1) = 1$ . Por otra parte  $\psi(a)$  es diferente de 0 si (a, m) = 1; en electo, determinando a' de la condición aa' =  $= 1 \pmod{m}$ , obtenemos  $\psi(a) \psi(a') = 1$ .

 $S_1(a_1, m) = 1$ , se tiene

$$\sum_{a} \frac{\chi(a)}{\psi(a)} = \sum_{a} \frac{\chi(a_1 a)}{\psi(a_1 a)} = \frac{\chi(a_1)}{\psi(a_1)} \sum_{a} \frac{\chi(a)}{\psi(a)}$$

per la cual, o  $\sum_{i=0}^{\infty} \frac{\chi(a)}{\psi(a)} = 0$  o bien  $\psi(a_i) = \chi(a_i)$  para todos los valo-

res de aj. Pero la primera proposición no puede verificarse para todos los  $\chi$ , pues en caso contrario seria H=0, mientras que  $H=\phi(m)$  ya que, sumando para un valor dado a respecto de todos los caracteres, se trene

$$\sum_{\alpha} \frac{\chi(\alpha)}{\psi(\alpha)} = \left\{ \begin{array}{ll} \phi(m), & \text{si } \alpha \equiv 1 \pmod{m}, \\ 0 & \text{en caso confrario.} \end{array} \right.$$

I.  $\alpha$ ) Si  $R'_1, \ldots, R_h$  y  $R''_1, \ldots, R'_h$  som los valores de  $R_1, \ldots, R_h$ , correspondientes a los caracteres  $\chi_1(a)$  y  $\chi_2(a)$  entonces  $\chi_1(a)$   $\chi_2(a)$  es el carácter cuyos valores correspondientes son R'R",

β) Cuando R, ..., Rk recorren todas las raices de las correspondientes equaciones,  $R'R_1$ , ...,  $R'_kR_k$  recorren en cierto orden las mismas rajoes.

y, Determinando l' de la condición  $ll' \equiv 1 \pmod{m}$ , se tiene

$$\sum_{\chi} \frac{\chi(a)}{\chi(l)} = \sum_{\chi} \frac{\chi(al')}{\chi(ll')} = \sum_{\chi} \chi(al').$$

lo cual es igual a  $\phi(m)$  o a 0, según que sea  $a = l \pmod{m}$  o no. 10, a, a) Determinando x' mediante la congruencia  $xx' = l \pmod{\rho}$ , se tiene

$$\sum_{x=1}^{p-1} e^{2\pi i \frac{1 \ln d (x+h) - t \ln d x}{\pi}} = \sum_{x=1}^{-1} e^{\frac{x}{2\pi i t} \frac{t \ln d (t+hx')}{\pi}} = -1.$$

B) Se tiene

$$S = \sum_{x=0}^{p-1} \sum_{z_1=0}^{Q-1} \sum_{z=0}^{Q-1} \frac{2\pi i}{s} \frac{i \ln d (x+z_1)^{-1} \ln d (x+z)}{n},$$

Si  $z_1 = z$  la sumación respecto de x da p-t, si  $z_1$  no es igual a z la sumación respecto de x (pregunta x)) da -1. Por lo tanto,

$$S = Q(p-1) - Q(Q-1) = (p-Q)Q.$$

11, a. a) Se tiene

$$\begin{aligned} & \mathcal{U}_{n, p} \mid 3 = \sum_{i=1}^{p-1} \sum_{x=1}^{p-1} e^{2\pi i \frac{h \ln d \cdot t}{n}} e^{2\pi i \frac{a \cdot (t-1) \cdot x}{p}} = \\ & = \beta - 1 - \sum_{i=0}^{p-1} e^{2\pi i \frac{h \ln d \cdot t}{n}} = p. \end{aligned}$$

β) Si (a, p) = p, el teorema es evidente. Si (a, p) = 1, el teorema se deduce de

$$U_{a, p} = e^{2\pi i \frac{-h \ln a}{n}} \sum_{x=1}^{p-1} e^{2\pi i \frac{h \ln a}{n}} e^{2\pi i \frac{ax}{p}} = e^{2\pi i \frac{-h \ln a}{n}} U_{1, p}.$$

γ) Evidentemente, A y B son enteros  $y \mid S \mid = A^3 + B^3$ . Para cierlos ε, ε', ε' que cumplen la condición |ε| = |ε'| = ε'' |= 1, se tiene (pregunta β)

$$S = \frac{1}{\epsilon \sqrt{p} \cdot \sqrt{p}} \sum_{\substack{z_1 = 1 \ z_1 = 1}}^{p-1} \sum_{x_1 = 1}^{p-1} \sum_{x_2 = 0}^{2\pi i} e^{\frac{\ln d \cdot z_1 + \ln d \cdot z}{k}} 2\pi i \frac{z_1 x + z_2 (x + 1)}{p}.$$

Si  $z_1 + z$  no es igual a p, la sumación respecto de x da cero. Por lo tante

$$S = \varepsilon' \sum_{n=1}^{p-1} \left( \frac{z}{p} \right) e^{2\pi i \frac{z}{p}} = \varepsilon' \sqrt{p}, \quad |S|^2 = p.$$

a) Se tiene

$$S = \frac{1}{n} \sum_{n=1}^{p-1} \sum_{k=1}^{n-1} e^{2\pi i \frac{k (\ln k \pi - k)}{n}} e^{2\pi i \frac{\pi}{p}}$$

La parte de esta expresión que corresponde a k=0, es igual  $a=\frac{1}{n}$ . La parte que corresponde a todos los valores positivos de k es en valor absoluto menor que (pregunta  $\alpha$ ))

$$\left(1-\frac{1}{n}\right)\sqrt{\rho}$$
.

b.  $\infty$ ) Para un valor de z dado, la congruencia  $z^n = z \pmod{p}$  es posible solamente cuando ind z es divisible por  $\delta$ , teniendo en este caso  $\delta$  soluciones. Por lo tanto

$$S_{\sigma, p} = 1 + \delta \sum_{n} e^{2\pi i \frac{\alpha n_0}{p}} = \delta \left( \frac{1}{\delta} + \sum_{n} e^{2\pi i \frac{\alpha n_0}{p}} \right),$$

donde  $z_0$  recorre los números del sistema reducido de restos respecto del módulo p que cumplen la condición ind z=0 (mód. 8). Por lo tanto (pregunta a, 8))

$$S_{a,p} < \delta \left(1 - \frac{1}{\delta}\right) \sqrt{\rho} = (\delta - 1) \sqrt{\rho}.$$

B) Haclendo

$$x = u + p^{s-1}v$$
;  $u = 0, ..., p^{s-1} - 1, v = 0, ..., p - 1,$ 

se tiene

$$e^{2\pi i \frac{\alpha n^n}{p^s}} = e^{2\pi i e (u^n p^{-s} + nu^{n-1} p^{-1} v)}$$

Si (u, p) = 1 la sumación respecto de v de cero. Por lo tanto

$$S_{a, p^{i}} = \sum_{n=0}^{p^{i-1}-1} e^{2\pi i a p^{n-i} x_{0}^{n}} = p^{i-1}, \quad S'_{a, p^{i}} = 0.$$

γ) Sea  $p^{\tau}$  la máxima potencia de p que divide a n. Se tiene  $s \gg \tau + 3$  Haciendo

 $x = u + p^{p-1-\tau}v$ ,  $u = 0, \ldots, p^{p-1-\tau} - 1$ ,  $v = 0, \ldots, p^{\tau+1} - 1$ , obtained

$$e^{2\pi i \frac{ax^n}{p^4}} = e^{2\pi i a \left(u^n p^{-2} + nu^{n-1} p^{-4} - i_0\right)}.$$

 $S_{i}(u, p) = 1$  la sumación respecto de v da cero. Por lo tanto

$$S_{a, p^{4}} = \sum_{x_{0}=0}^{p^{4}-1} e^{\frac{2\pi i}{p^{4}-n_{1}}} = p^{n-1}S_{a_{4}p^{4}-n_{1}} S'_{a_{1}p^{4}} = 0$$

ð) Sea  $m=
ho_1^{m_1}$  .  $ho_k^{m_k}$  la descomposición canónica del número n Haciendo

$$T_{a, m} = m^{-1+\nu} S_{a, m}; \quad \mathbf{v} = \frac{1}{n}, \quad m = M_1 p_1^{\alpha_1} = \dots = M_k p_k^{\alpha_k}$$

y determinando as, ..., ah de la condición

$$a = M_1a_1 + \ldots + M_ha_h \pmod{m}$$
,

se liene (pregunta 12, d, cap. iii)

$$T_{a_1 \cdot m} = T_{a_1 \cdot p_1^{m_1}} \cdot \cdot \cdot \cdot T_{a_k \cdot p_k^{m_k}}$$

Pero, at a= 1, se tiene

$$|T_{q, p^{i}}| < p^{mi+\eta} n \sqrt{p} < np^{-\frac{1}{6}}$$

St 1 < s < n, (a, p) = 1, so tiene

$$|T_{a_i,p^k}| = p^{-k+av}p^{i-1} \le 1.$$

Si 1 < s < n, (a, p) = p, se tiene

$$|T_{a,p^k}| < p^{-n+s\nu}p^s < p < n.$$

El caso a > n, en virtud de que  $T_{a, p^a} = p^{-a+nv}p^{n-1}S_{a, p^a-n} = T_a, p^{a-n}$  se reduce al caso a < n. Por lo tanto

$$|T_{a,m}| \le C = n^{n+n}$$
.

de donde se deduce la desigualdad indicada en la pregunta.

12, a. Se deduce del teorema de la pregunta II, a, cs) y del teorema de la pregunta I2, a, cs) cap. V.

b, a) Se tjene

$$Tn = \sum_{n=M}^{M+Q-1} \sum_{h=0}^{n-1} e^{2\pi i \frac{h \left(\ln d \cdot x - s\right)}{n}}.$$

Para k=0, aumando respecto de x, resulta Q, para k>0 resulta un número cuyo módulo es menor que  $\sqrt{\rho}$  in  $\rho$ . De aqui se deduce la fórmula indicada en la pregunta

β) Se deduce del teorema de la pregunta 12, a, β) cap V y del teorema de la pregunta 11, a, δ).

c. Tomando f(x) = 1, si x recorre los valores  $x = \inf M$ , and (M + 1)..., ind (M + Q - 1), results (pregunts 17, a, cap. II)  $S' = \sum_{d \in P - 1} \mu(d) S_d$ .

Aqui S' es el numero de valores de x que cumplen la condicion (x, p-1) = 1,

por le tante, S' = H. Per etra parte,  $S_d$  es el número de valores de x que son múltiples de d, es decir, es el número de restes de grado d que hay en la sucesión M, M+1, ..., M+Q-1. Per consiguiente,

$$H = \sum_{d \mid p-1} \mu(d) \left( \frac{Q}{d} + \theta_d \sqrt{\rho} \ln \rho \right); \quad |\theta_d| < 1, \quad \theta_0 = 0.$$

$$\sum_{z}' \Phi(z) = J, \quad \sum_{z} \Phi(z) = Q, \quad J = \frac{Q_{z}}{p-1} Q + \theta \sqrt{p} (\ln p)^{2}$$

13. Supongamos que no hay no-restos no superiores a h. La cantidad de po-restos de grado n que hay entre los números

1, ..., 
$$Q$$
;  $Q \Rightarrow [\sqrt{p} (\ln p)^2]$ 

se puede acotar de dos modos:

Partiendo de la fórmula de la pregunta 12, b y teniendo en cuenta que pueden ser no restos solamente los números que son divinibles por números primos mayores que h. Resulta

$$1 - \frac{1}{n} < \ln \frac{\frac{1}{2} \ln \rho + 2 \ln \ln \rho}{\frac{1}{c} \ln \rho + 2 \ln \ln \rho} + O \frac{1}{\ln \rho}.$$

$$0 < \ln \frac{1 + 4 \frac{\ln \ln \rho}{\ln \rho}}{1 + 2c \frac{\ln \ln \rho}{\ln \rho}} + O \left(\frac{1}{\ln \rho}\right).$$

La imposibilidad de la última desigualdad para todos los números p suficientemento grandes demuestra el teorems.

14, a. Se tiene

$$\mid S\mid^2\leqslant X\sum_{m=0}^{m-1}\sum_{y_1=0}^{m-1}\sum_{y_2=0}^{m-1}\rho\left(y_1\right)\overline{\rho\left(y\right)}\;e^{\frac{2\pi i}{m}}\frac{\alpha x\left(y_1-y\right)}{m}$$

Para valores dados de  $y_1$  e  $y_2$  la sumución respecto de x da  $Xm \mid \rho(y) \mid k$  o cero, según que sea  $y_1 = y$  o no. Por lo tanto

$$|S|^2 \leqslant XYm$$
,  $|S| \leqslant \sqrt{XYm}$ .

b, α) Se tiene

$$S = \frac{1}{\varphi(\langle u \rangle)} \sum_{u} \sum_{\sigma} \chi(u) \chi(\sigma) e^{2\pi i \frac{\alpha u^{\sigma} e^{\pi}}{m}},$$

donde u y v recorren los sistemas reducidos de restos respecto del módulo m. De aqui que

$$S = \frac{1}{\varphi(m)} \sum_{m=0}^{m-1} \sum_{y=0}^{m-1} v(x) \rho(y) e^{2\pi i \frac{dxy}{m}};$$

$$v(x) = \sum_{\substack{u^n = x \pmod{d, m}}} \chi(u), \quad \rho(y) = \sum_{\substack{u^n = x \pmod{d, m}}} \chi(v)$$

Pero, se tiene (pregunta 11, cap. IV)

$$\sum_{x=0}^{m-1} |v(x)|^{\frac{n}{2}} \le K\varphi(m), \quad \sum_{y=0}^{m-1} |\rho(y)|^{2} \le K\varphi(m).$$

Por lo tanto (pregunta a)

$$|S| < \frac{1}{\varphi(m)} \sqrt{K\varphi(m) K\varphi(m) m} = K \sqrt{m}$$

β) Sea  $m = 2^{\alpha}p_1^{\alpha_1} \dots p_n^{\alpha_n}$  la descomposición canónica del número m. La congruencia  $x^n \equiv 1 \pmod{m}$  es equivalente al sistema

$$x^n \equiv 1 \pmod{2^n}, \quad x^n \equiv 1 \pmod{p_k^{n_1}}, \dots, \quad x^n \equiv 1 \pmod{p_k^{n_k}}.$$

$$K \leq 2 \left(\tau(m)\right)^{\frac{\ln n}{\ln 2}}; \quad K = O(m^6).$$

c. a) Pácilmente se observe que a recorre

$$U = (p-1)\left(1+\frac{1}{q_k}\right)\dots\left(1+\frac{1}{q_h}\right)^{\frac{1}{2}-h}$$

valores, y a' recorre

$$V = (\rho - 1) \left(1 - \frac{1}{q_k}\right) \dots \left(1 - \frac{1}{q_k}\right)^{2^{-k}}$$

valores. Además, cuando t, para unos valores dados de s y s', recorre el sistema reducido de restos respecto del módulo p-1, el producto (s+s') t también recorre el sistema reducido de restos respecto del módulo p-t. Por lo tanto, W=UVS. Pero, en virtud del teorema de la pregunta a, se tiene  $|S_1| < VUVp$  y, por consiguienta, W=-p (p-1) VUVp. Comparando las dos expresiones halladas para W, se obtiene

$$S < \varphi(p-1) \sqrt{\frac{p}{UV}} = \frac{\varphi(p-1)}{p-1} \frac{2^{k} \sqrt{p}}{\sqrt{\left(1 - \frac{1}{q_{k}^{T}}\right) \cdot \cdot \left(1 - \frac{1}{q_{k}^{T}}\right)}} < \frac{9}{8} \frac{\varphi(p-1)}{p-1} 2^{k} \sqrt{p}.$$

β) Se deduce del teorema de la pregunta 12, a, α) cap. V y del teorema de la pregunta α).

 $\gamma$ ) Se deduce del teorema de la pregunta 12, a,  $\beta$ ) cap. V y del teorema de la pregunta  $\alpha$ ).

15, a. Se tiene

$$|S|^{3} = \sum_{i=1}^{p-1} \sum_{x=i}^{p-1} e^{3\pi i \frac{a(i^n-1)x^n+b(i-1)x}{p}}$$

En el caso  $t^n = 1 \pmod{p}$ , la aumación respecto de x da p-1 si t=1 y -1 si t>1. En el caso contrario, tomando  $z(t-1)^{-1}$  en lugar de x la parte de la suma doble que corresponde al valor t elegido la expresamos en la forma

$$\sum_{i=1}^{p-1} e^{2\pi i \frac{\alpha(t^n-1)(t-1)^{-n}x^n+bx}{p}}.$$

Por lo tanto

$$|S|^2 \leqslant \rho - 1 + \Big|\sum_{1}^{p-1} \sum_{1}^{p-1} \forall (u) \ \rho \ (v) \ a^{\frac{2\pi i}{p}} \Big|,$$

donde v(u) no es superior al número de soluciones de la congruencia  $(t^n-1)(t-1)^{-n} \equiv u \pmod{p}$  con la condición t > 1,  $y \mid p(v) \mid$  no es superior al número de soluciones de la congruencia  $z^n \equiv v \pmod{p}$ .

Por lo tanto,  $v(u) \leq 2n_1$ ,  $\rho(v) | \leq n_1$ ,

$$\sum_{u=-1}^{p-1} (v(u))^2 \leqslant (p-1) \, 2n_1, \quad \sum_{v=-1}^{p-1} |p(v)|^2 \leqslant (p-1) \, n_1.$$

Aplicando el teorema de la pregunta 14, a, obtenemos

$$|S|^2 \leqslant p-1+\sqrt{(p-1)}\frac{2n_1(p-1)n_1p}{2n_1(p-1)n_1p} \leqslant 2n_1p^{\frac{3}{2}}$$

b, a) So deduce del teorema de la pregunta a y del teorema de la pregunta (2, a, a) cap. V,

β) Del teorema de la pregunta α) se deduce que se cumplen las condiciones del teorema de la pregunta 12, a, α) cap. V si se hace m = p.

 $\Phi(z) = 1$ ,  $\Delta = \frac{3}{2} n_1^{\frac{1}{2}} \rho^{\frac{3}{4}} \ln \rho$ , y z recorre los valores  $z = Ax^n$ ;  $x = M_0$ ,

 $M_0 + l_1 \dots M_0 + Q_0 + l$ . Por lo tanto

$$\sum_{z}' \Phi(z) = T, \qquad \sum_{z} \Phi(z) = Q_{0},$$

de donde se deduce la fórmula indicada en la pregunta.

c,  $\alpha$ ) Supongamos que  $\gamma = 4\alpha\gamma_1 \pmod{p}$ . Se tiene (pregunta 11, a, cap. V)

$$\left(\frac{a}{p}\right)S = \sum_{n=0}^{p-1} \left(\frac{4a^3x^2 + 4abx + 4ac}{p}\right) e^{2\pi i \frac{4a^3x^2 + 4abx + 4ac}{p}} = \frac{1}{U_{1, p}} \sum_{n=1}^{p-1} \left(\frac{2}{p}\right) \sum_{n=0}^{p-1} e^{2\pi i \frac{x(6a^3x^3 + 4abx + 4ac + 4a\gamma_1xx^{-1})}{p}} = \sum_{n=0}^{p-1} e^{2\pi i \frac{x(6a^3x^3 + 4abx + 4ac + 4a\gamma_1xx^{-1})}{p}} = \sum_{n=0}^{p-1} e^{2\pi i \frac{x(6a^3x^3 + 4abx + 4ac + 4a\gamma_1xx^{-1})}{p}}$$

La última suma es en valor absoluto (pregunta a)  $< \frac{3}{2} p^{\frac{3}{4}}$ 

β) Se deduce del teorema de la pregunta α) y del teorema de la pregunta (2, α, α) cap.  $V_*$ 

# Respuestas a los ejercicios numéricos

#### Respuestas a los ejercicios del capitalo i

2, a. a) 
$$\delta_4 = \frac{16}{11}$$
; b)  $\alpha = \frac{19}{14} + \frac{\theta}{14 \cdot 20}$ .

b. a) 
$$\delta_8 = \frac{80}{59}$$
;  $\beta$ )  $\alpha = \frac{1002}{739} + \frac{\theta}{739 \cdot 1000}$ .

3. En total se obtlenen 22 fracciones

#### Respuestas a los ejercicios del capitulo li

1, a. 1312.

$$\times \quad \textbf{47$^{\circ}} \cdot 53^{\circ} \cdot 59^{\circ} \cdot 61^{\circ} \cdot 67 \cdot 71 \cdot 73 \cdot 79 \cdot 83 \cdot 89 \cdot 97 \cdot 101 \cdot 103 \cdot 107 \cdot 109 \cdot 113.$$

2, a, 
$$\tau$$
 (5600) = 36; S (5600) = 15 624.

**b.** 
$$\tau$$
 (116 424) = 96; S (118 424) = 410 400.

#### Respuestas a los ejercicios del capitulo III

#### Respuestas a tos ejercicios del capituto IV

- 1, a. x = 81 (mod 337), b. x = 200, 751, 1302; 1853; 2404 (mod 2755).
- 2. b. x = 1630 (môd 2413).
- 3. x = 94 + 111 t, y = 39 + 47 t, donde t es un entero arbitrario.
- 4. a. x = 170b, + 52b, (mód. 22i).
  - $x = 131 \pmod{221}, x = 110 \pmod{221}; x = 89 \pmod{221}.$ 
    - **b.**  $x = 11 \cdot 151b_1 + 11 \cdot 800b_2 + 16 \cdot 875b_3 \pmod{39 \cdot 825}$
- 5, a. x = 91 (mód. 120) b. x = 8479 (mód. 15 015)
- x = 100 (mód, 143), y = 111 (mód, 143)
- 7. a.  $3x^4 + 2x^9 + 3x^9 + 2x = 0 \pmod{5}$ .
  - **b.**  $x^3 + 5x^4 + 3x^3 + 3x + 2 = 0 \pmod{7}$ .
- 8.  $x^6 + 4x^6 + 22x^6 + 76x^6 + 70x^6 + 52x + 39 = 0 \pmod{101}$
- 9. a. x = 16 (mód 27), b. x = 22, 53 (mód 64)
- 10. a. z = 113 (mód. 125).
  - b. z 43, [23, 168, 248, 293, 373, 418, 498, 543, 623, (mód. 625).
- ft. a. x = 2, 5; 11, 17, 20, 26 (mod 30),
  - b. x = 76, 22, 176, 122 (mód. 225),

#### Respuestas a los ejercicios del capitulo V

- 1, s. 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18.
  - b. 2, 6, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35.
- 2, a. α) 0; β) 2, b. α) 0; β) 2, 8, a. α) 0; β) 2. b.α) 0; β) 2.
- 4, a. a)  $x = \pm 9 \pmod{19}$ ; b)  $x = \pm 11 \pmod{29}$ ;
  - $y) \times m \pm 14 \text{ (mod. 97)}.$
  - **b.** a)  $x = \pm 68 \pmod{311}$ ; b)  $x = \pm 130 \pmod{277}$ ;
  - $\gamma$ )  $\kappa = \pm 94 \pmod{353}$ .
- 5, a.  $x = \pm 72$  (mod. 125). b.  $x = \pm 127$  (mod. 243).
- 0, a. x = 13, 19, 45, 51 (mod. 64), b. x = 41, 87, 169, 215 (mod. 256)

#### Respuestos a los ejercicios del capitalo Vi

- 1, 4, 6, 5, 18
- 2, a. 3, 3, 3. b. 8, 5, 5. c. 7.
- 5, a. α) 0; β) 1; γ) 3. b. α) 0; β) 1; γ) 10.
- 6, a. a) x = 40; 27 (mód. 67), β) x = 33 (mód. 67).
  - y) x = 8, 36, 28, 59, 31, 39 (mod 67)
  - **b.** a)  $x = 17 \pmod{.73}$  b)  $x = 50, 12, 35, 23, 61, 38 \pmod{.73}$ . γ) x = 3, 24, 46 (mód. 73).

- 7, a. a) 0; b) 4. b. a) 0; b) 7.
- 8, a. α) x = 54 (mód. 101) β) x = 63, 86, 90, 66, 8 (mód. 101). b. x = 59, 11, 39 (mód. 109).
- 9, a. α) 1, 4, 5, 6, 7, 9, 11, 16, 17; β) 1, 7, 8, 11, 12, 18. b. α) 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36;
  - β) 1, 7, 9, 10, 12, 16, 26, 33, 34,
- 10, a. a) 7, 37; β) 3, 5, 12, 18, 19, 20, 26, 26, 29, 30, 33, 34.
  - b. a) 3, 27, 41, 52;
    - β) 2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59

### TABLAS DE INDICES

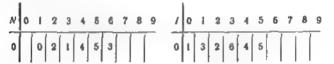
NUMERO PRIMO 3	NU	MERC	PRI	MO 3
----------------	----	------	-----	------

- 1						1						
0	0	1				0	1	2				

#### NUMERO PRIMO 5

N	0	1	2	3	4	5	6	7	8	9	1	0	1	2	3	4	б	6	7	8	9
0		0	1	3	2						0	L	2	4	3						

#### **NUMERO PRIMO ?**



#### NUMERO PRIMO II

											/										
0	Б	0	1	8	2	4	9	7	3	6	0	1	2	4	8	5	10	9	7	3	6

W 0																				
0 10	0 7	6	4	2	9	5	11	3	8	0	10	7	4	8	3	6	12	11	9	5

NUMERO	PRIMO	17
1		

NUMERO PRIMO 17	
N 0 1 2 3 4 5 6 7 8 9	10123456789
0 14 1 12 5 15 11 10 2	0 1 3 9 10 13 5 15 11 16 14 1 8 7 4 12 3 6
NUMERO PRIMO 19	
N 0 1 2 3 4 5 6 7 8 9	10123456789
0 1 13 2 16 14 6 3 8 1 17 12 15 5 7 11 4 10 9	0 1 2 4 8 16 13 7 14 9 18 1 17 15 11 3 6 12 5 10
NUMERO PRIMO 23	
N 0 1 2 3 4 5 6 7 6 9	10123456789
0 0 2 16 4 1 18 19 6 10 1 3 9 20 14 21 17 8 7 12 15 2 5 13 11	0   1   5   2   10   4   20   8   17   16   11   1   9   22   18   21   13   19   3   15   6   7
NUMERO PRIMO 29	
N 0 1 2 3 4 5 6 7 8 9	/ 0 l 2 3 4 5 6 7 8 9
0 0 1 5 2 22 6 12 3 10 1 23 25 7 18 13 27 4 21 11 9 2 24 17 26 20 8 16 19 15 14	0 1 2 4 8 16 3 6 12 24 19 1 9 18 7 14 28 27 25 21 13 26 2 23 17 5 10 20 11 22 15
NUMERO PRIMO 31	
N 0 1 2 3 4 5 6 7 8 9 0 0 24 1 18 20 25 28 12 2 1 14 23 19 11 22 21 6 7 26 4 2 8 29 17 27 13 10 5 3 16 9	/ 0 1 2 3 4 5 6 7 8 9  0 1 3 9 27 19 26 16 17 20 29 1 25 13 8 24 10 30 28 22 4 12 2 5 15 14 11 2 6 18 23 7 21

#### NUMERO PRIMO 37

0 1 2 3	24 25 14	0 30 22	28 31 5	26 11 15 20	2 33 29 8	23 13 10 19	27 4 12 18	32 7 6	3 17 34	16 35 21	0	1 25 33 11	2 13 29 22	26 21 7	8 15 5 14	16 30 10 28	32 23 20 19	27 9 3	17 18 6	34 36 12	31 35 24

#### NUMERO PRIMO 41

N	0	1	2	3	4	5	6	7	8	9	1	0	1	2	3	4	5	6	7	8	9
3	8 34	3 14 28	27 29	31 36	12 25 13 19	37 4	24 17	33 5	16 11	9	1 2	32 40	28 35	36 4 5 37	24 30	21 16	3 14	18	26 12	33 31	34 22

#### NUMERO PRIMO 43

N	0	1	2	3	4	5	6	7	8	9	1	0	1	2	3	4	5	6	7	8	9
2	10 37	36 34	15	32 16 31	20 40	26 8	17	38 3	29 5	19	2	14	30 42 33 29	4 40	12 34 30	36 16	22 5 7	23 15 21	26	25 35 6 17	19

<b>"</b>		_						7				0	1	2	3	4	5	6	7	8	9
0 1 2 3 4	19 37 39	6 3	10 25 44	11 5 27	28 34	21 2: 33	26	16 14 42	12	45 35	2 3	3 36	5 13 15 39 45	28 7	43 46 35	27 42 34	41 22 29	17 16 4	38	2 24	10

NTIM	ERO	PRI	MO.	53

N	0	1	2	3	4	5	6	7	8	9								6			
0		0	- 1	17	2	47	18	14	3	34 37 46	0		2	4	8	16	32	11 28	22	44	35
1	42	6	19	24	15	12	4	10	35	37	1	17	34	15	30	7	14	28	3	6	12
2	49	31	7	39	20	42	25	51	16	46	2	24	48	43	33	13	26	52	51	49	45
3	13	33	5	23	11,	9	36	30	38	41	3	37	21	42	31	9	18	36	19	38	23
- 4	50	45	32	22	8	29	40	44	21	41 28	4	46	39	25	50	47	41	29	5	10	20
5	43	27	26								5	40	27								

#### NUMERO PRIMO 59

N				3							_				-		_	6			
0				50							0	1	2	4	8	16	32	5	10	20	40
				45														46			
				15														22			
				17														49			
				33														26			
5	13	32	47	22	35	31	21	30	29		5	3	6	12	24	48	37	15	30		

#### NUMERO PRIMO 61

												1										
N	0	1	2	3	4	5	6	7	8	9	- /	10	)	1	2	3	4	5	6	7	8	9
0		0	-1	6	1			49			0		ī	2	4	8	16	32	3	6	12	24
	23			40							ì	4	8	35					22			
			16								- 2	4	7	33	5	10	20	40	19	38	15	30
		_	- 5								3	6	o	59	57	53	45	29	58	55	49	37
			56								4	ŀΙι	3	26	52	43	25	50	39	17	34	. 7
5	45	53	42	33	19	37	52	32	36	31									42			
6	30											Τ,	1				- 0		1-		7.4	

N		1	2	3	4	5	6	7	8	9	1	0	1	2	3	4		-	7	8	9
0				39							0	i	2					64			
L	16	59	41	19	24	54	- 4	64	13	10	I)	19	38	9	18	36	5	10	20	40	13
2	17	62	60	28	42	30	20	51	25	44								56			
3	55	47	5	32	65	38	14	22	11,	58	3	25	50	33	66	65	63	59	61	J5	3
				9														49			
5	31	37	21	57	52	8	26	49	45	36	5	47	27	54	41	15	30	60	53	39	11
6	56	- 7	48	35	6	34	33				6	22	44	21	42	17	34				

#### 200 TABLAS DE INDICES

#### NUMERO PRIMO 71

N	0	1	2	3	4	5	.6	7	8	9	1	0	1	2	3	4	5	6	7	8	9
3644	34 40 50 46 52	31 27 11 25 5	38 37 30 33 51	39 16 57 48 23	12 7 44 55 43 14 36	56 29 10 59	24 45 64 21	49 8 20 9 42	58 13 22 50	16 68 65 2 3	1 2 3 4 5	45 37 32 20 48	31 46 11 69 52	49 4 38 6 57 9	59 28 53 42 44 63	58 54 16 10 24 15	51 23 41 70 26 34	2 19 3 64 40 25	14 62 21 22 67 33	27 8 5 12 43	56 35 13 17 55

#### NUMERO PRIMO 73

N	0	ì	2	3	4	5	6	7	8	9	i	0	1	2	3	4	5	6	7	8	9
0	Н	0			16		14				0		5	25	52	41	59	3	15	2	10
-1	9	55	22	59	41	7	32	21	20	62		50	31	9	45	- 6	30	- 4	20	27	62
2	17	39	63	46	30	2	67	18	49	35	2	18	17	12	60	-8	40	54	51	36	34
3	15	11	40	61	29	34	28	64	70	65	3	24	47	16	7	35	29	72	68	48	21
4	25	-4	47	51	71	13	54	31	38	66	4	32	14	70	58	71	63	23	42	64	28
5	01	27	3	53	26	56	57	68	43	5	5	67	43	69	53	46	11	55	56	61	13
6	23	58	19	45	48	60	69	50	37	52	6	65	33	19	22	37	39	49	25	57	66
7	42	44	36			-		Į			7	38	44							1	

N.	a	1	2	3	4	5	ő	7	đ	9	1	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	Б	53	12	2	0	1	3	9	27	2	6	18	54	4	12
-1	66	68	9	34	57	63	16	21	6	32										65	
					13															49	
					25						3	46	59	19	57	13	39	38	35	26	78
					76															67	
5	50	22	42	77	7	52	65	33	15	31										42	
6	7 l	45	60	55.	24	18	73	48	29	27	6	62	28	5	15	45	56	10	30	12	33
7	41	51	14	44	23	47	40	43	39		7	20	60	22	66	40	41	44	53		

M	1.04	FP	O.	PD	IMO	8.3

N	0	1	2	3	4	5	6	7	8	9	,	0	1	2	3	4	5	6	7	8	9
III :		0	1	72		27	73	8	3	62	0	1	2	4	8	16	32	64	45	7	14
-1	28	24	74	77	9	17	-4	56	63	47	L	28	56	29	58	33	66	49	15	30	60
2	29	80	25	60	75	54	78	52	10	12	2	37	74	65	47	11	22	44	- 5	10	20
3	118	38	Б	14	57	35	64	20	48	67	3	40	80	77	71	59	35	70	57	31	62
4	30	40	81	71	26	7	61	23	76	16	4	41	62	81	79	75	67	51	19	38	76
5	55	46	79	59	53	51	Ш	37	13	34	5	69	55	27	54	25	50	17	34	68	53
6	19	66	39	70	6	22	15	45	56	50		23		9	18	36	72	61 48	39	78	73
7	36	33	65	69	21	44	49	32	68	43	7	63	43	3	6	12	24	48	13	26	52
8	31	42	41		-						8	21	42			i	ŀ	- [			

#### NUMERO PRIMO 89

N	0	1	2	3	4	5	6	7	8	9	7	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48		0	1	9	0	27	91	65	17	51	64	14
	86				9						ĭ	42	37	22	66	20	60	2	6	18	54
2	14	82	12	57	49	52	39	3	25	59	2	73	41	34	13	39	28	84	74	44	43
3	87	31	80	85	22	63	34	П	51	24	3	40	31	- 4	12	36	19	57	82	68	26
4	30	21	10	29	28	72	73	54	65	74	4	78	56	79	59	88	86	80	62	6	24
5	68	7	55	78	19	66	41	36	75	43							52				
6	15	69	47	83	8 27	5	13	56	38	58							48				
7	79	62	50	20	27	53	67	77	40	42	7	5	15	45	46	49	58	85	77	53	70
8	46	4	37	61	26	76	45	60	44		8	32	7	21	63	11	33	10	30		

				2	4	E	6	7	В	0	,	l,		9	7	4	E	6	7		0
N	U.		2	3	-	5	6			9	<u>.</u>	۳,		- 2	3	-				-	- 3
0		0	34	70	68	1	8	31	6	44	0	1	5	25	28	43	21	8	40	6	30
1	35	86	42	25	65	71	40	89		81	1	53	71	64		48	46	36	83		
2	69	5	24	77	76	2	59	18	3		2	93	77			22		65			
3	9	46		60							3	79	7	35	78	2		50			
4	7	85	39	4	58	45	15	84	14	62	4	16	80	12	60	9	45	31	58	96	92
5	36	63	93	10	52	87	37	55	47	67	5	72						91			26
6	43	64	80	75			94				6	33	68	49	51	61	14	70	59	- 4	20
7	66	11	50	28	29	72	53	21	33	30	7	3	15	75	84	32	63	24	23	18	
8	41	88	23	17	73	90	38	83	92	54	8		19	95	87	47	41	11	55	81	17
	79	56	49	20	22	82	48		- 1		9	85	37	88	52	66	39		-		

TABLA de los números primos <4070 y sus raíces primitivas mínimas

p	£	٥		P	4	р		p	E	p		p	E
23 56 7	1 2 2 3 2	179 181 191 193 197	2292	419 421 431 433 439	22755	661 673 677 683 691	26253	947 963 967 971 977	2 3 5 6 3	1229 1231 1237 1249 1259	2322	1523 1531 1543 1549 1863	Caro Or NO to
13 17 19 23 29	3 2 2 2	199 211 223 227 229	23396	448 449 457 481 463	12	701 709 719 727 733	1196	983 991 997 1009 1013	6 7 11 8	1277 1279 1283 1289 1291	20000	1559 1567 1571 1579 1583	19 3 3 5
31 41 43 47	3 6 3 6	233 239 241 251 257	7783	467 479 487 491 499	2 13 2 7	739 743 751 757 761	3 6 3 4 6	1019 1021 1031 1033 1039	10 14 6 3	1297 1301 1303 1307 1319	10 6 2 13	1597 1601 1607 1609 1613	11 8 7 3
63 80 61 67 71	2 2 2 7	253 269 271 277 281	6 2 6 5 3	503 509 521 523 541	**********	780 773 787 787 787 809	1-2222	1049 1051 1061 1063 1069	3 7 2 3 6	1321 1327 1361 1367 1373	200000	16(9 1621 1627 1637 1657	22.33
73 79 63 69 97	3 3 5	263 293 307 311 313	170	547 557 563 569 571	New Sea	811 821 823 827 829	3 2 2 2	1087 1091 1093 1097	3 2 5 5 5	1381 1399 1409 1423 1427	13332	1668 1667 1669 1693 1697	32203
101 103 107 109 113	2 6 3	317 331 337 347 349	22040	577 567 593 599 601	52377	839 853 857 859 863	3 2 5	1109 1117 1123 1129 1181	2 11 17	1429 1433 1439 1447 1451	5373N	1699 1709 1721 1723 1733	38333
127 131 137 139 149	3 2 3 2	358 359 367 373 279	77-6 M M	607 613 617 619 631	200000	877 881 883 867 907	3 3 5 3	1163 1163 1171 1101 1187	5 2 7 2	1453 1459 1471 1481 1483	5 5 3 2	1741 1747 1753 1789 1777	9 7 6 6
161 167 163 167 173	5 2 5 2	383 389 397 401 409	5 5 3 21	641 643 647 653 659	11 6 3	911 919 929 937 941	7 3 5 2	1193 1201 1213 1217 1223	3 11 2 3 5	1487 1489 1493 1499 1511	5 14 2 2	1783 1767 1769 1801	10

#### Continuación

								4		ld			
p 	£	P	£	p	e	p	E	р		P	£	P	ε
1823 1831 1847 186. 1867	53522	2131 2137 2141 2143 2153	3 3 10 2	2437 2441 2447 2459 2467	200000	2749 2753 2767 2777 2789	6 3 3 3	3083 3089 3109 3119 3119	2 3 6 7	3433 3449 3467 3461 3463	5 3 7 2 3	3733 3739 3761 3767 3769	7 3 5 7
1871 1873 1877 1879 1889	14 10 2 6 3	216! 2179 2203 2207 2213	23 7 5 5	2473 2477 2503 2521 2531	5 2 7 2	2791 2797 2801 2803 2619	8 2 3 2 2 2	3137 3163 3767 3.69 3181	3 5 7 7	3467 3469 3491 3499 3511	20207	3779 3793 3797 3803 3821	2 2 2 3
1901 1907 1913 193! 1933	212121212	2221 2237 2239 2243 2251	22327	2539 2543 2649 2651 2657	25369	2833 2837 2843 2851 2667	5 2 2 2 1 1	3187 3191 3203 3209 3717	21235	3517 3527 3529 3533 3539	2 5 17 2 2	3833 3833 3847 3861 3853	3 5 2 2
1949 1961 1973 1979 1987	3 2 2 2	3267 2269 2273 2261 2267	3719	2570 2591 2593 2609 2617	C1 C2 - 7 - 470	2861 2679 2867 2867 2897 2903	27635	3221 3229 3251 3253 3257	6 6 3	3541 3547 3557 3559 3571	7 2 3 3 2	3863 3677 3681 3689 3907	3 1 2
1993 1997 1999 2003 2011	5 2 3 5 3	2293 2207 2309 2311 2333	26232	2621 2633 2647 2657 2657 2659	200	2909 2917 2927 2939 2953	13	3259 3271 3299 3301 3307	32560	3581 3583 3593 3607 3613	23352	3911 3917 3919 3923 3929	1323
2017 2027 2029 2039 2053	52272	2339 2341 2347 2351 2357	2 7 3 13	2663 2671 2677 2683 2687	57226	2957 2963 2969 297. 2999	2 3 10 17	9313 3319 3323 3329 3331	10 6 2 3 3	3817 3623 3631 3637 3643	36598	3931 3943 3947 3967 3989	23 4 40 23
2063 2069 2081 2083 2087	5 2 3 2 5	2371 2377 2361 2363 2389	5 5 2	2689 2693 2699 2707 2711	192227	3001 3011 3019 3023 3037	14 2 2 6 2	3343 3347 3359 336, 3371	5 2 11 22 2	3659 3671 3673 3677 3691	23 6 2 2	4001 4003 4007 4013 4019	32500
2089 2099 211, 2113 2129	7 2 7 6 3	2393 2399 2411 2417 2423	3 11 6 3 5	2713 2719 2729 2731 2741	53332	3041 3049 3061 3067 3079	3 11 6 2 6	3373 3389 339: 3407 3413	5 3 5 2	3697 3701 3709 3719 3727	52273	4021 4027 4049 4051 4057	3355

#### INDICE ALFABÊTICO DE MATERIAS

Algoritmo de Euclides 16 Captidad de divisores de un número 36 Carácter 126 Clase de números respecto del módulo m 56 Coclente 14 Cocientes incompletos 22 Congruencia 52 Congruencia de primer grado 69 Congruencias binómicas 85 Congruencias de cualquier grado respecto de un módulo compues-Congruencias de cualquier grado respecto de un módulo pri-Congruencias equivalentes 68 Cribe de Eratostenes 26 Criterios de divisibilidad 60 Desarrollo en fracción conti-Descomposición canónica de un número 29 Divisor 13 Ecuación de Pell 103 Entero 13 Exponente a que pertenece un número respecto de un número 108 Fórmula de Sonin 42 Fracción continua 21 Fracciones reducidas 22 Función de Euler 37 Función de Móbius 36 Función [x] 33 Función (x) 33 Función  $\pi(x)$  48

Función  $\phi(x)$  43

Función (s) 45 Función 8 (s, s<sub>0</sub>) 43

Función multiplicative 34

Función T (a) 36

Lev reciproca de los reatos cuadráticos 91 Máximo común divisor 15 Mínimo común múltiplo 19 Módulo de una congruencia 52 Múltiplo Número compuesto 26 Número primo 26 Números congruentes 52 Números primos entre ai 15 Números primos entre si dos a dos 15 Raices primitivas respecto de un módulo 109 Residuo o resto 14 Resolución de una congruencia 68 Resto absoluto minimo 57 Resto (no resto) cuadrático, cúbico, bicuadrático, de grado Resto no negativo minimo 57 Resto respecto del módulo m 57 Símbolo de Jacobi 92 Símbolo de Legendre 87 Sistema completo de restos 57 Sistema de congruencias de primer grado 71 Sistema de indices de un número respecto del módulo 2ª 121 Sistems de Indices de un número respecto de un módulo compuesto 122 Sistema reducido de restos 58 Sucesión de Farey 30 Suma de divisores de un número 35 Tabla de números primos 202 Tablas de Indices 114, 115, 196-201 Teorema de Euler 59 Teorema de Fermat 60 Teorema de Wilson 74

Grado de una congruencia 68

Indice de un número 114

## INDICE

PROLOGO DEL TRADUCTOR	5
CAPITULO PRIMERO	
TEORIA DE LA DIVISIBILIDAD	
II. CONCEPTOS Y TEOREMAS FUNDAMENTALES	13
§ 2. MAXIMO COMUN DIVISOR	15
5 3. MINIMO COMUN MULTIPLO	19
4. RELACION DEL ALGORITMO DE EUCLIDES CON LAS FRAC-	
CIONES CONTINUAS	21
5 B. NUMEROS PRIMOS	25
5 6. UNICIDAD DE LA DESCOMPOSICION EN FACTORES PRIMOS	27
PREGUNTAS REFERENTES AL CAPITULO I	30
EJERCICIOS NUMERICOS REFERÊNTES AL CAPITULO I	32
CAPITULO SEGUNDO	
LAS FUNCIONES MAS IMPORTANTES DE LA TEORIA DE LOS NUMEROS	
t. FUNCIONES (z), (x)	33
2. SUMAS EXTENDIDAS A LOS DIVISORES DE UN NUMERO 3. FUNCION DE MOBIUS	34
4. FUNCION DE EULER	37
PREGUNTAS REFERENTES AL CAPITULO II	39
EJERCICIOS NUMERICOS REFERENTES AL CAPITULO 11	51
CAPITULO TERCERO	
CONGRUENCIAS	
I. CONCEPTOS FUNDAMENTALES	52
2. PROPIEDADES DE LAS CONGRUENCIAS, SEMEJANTES A LAS	-
PROPIEDADES DE LAS IGUALDADES	53
3. OTRAS PROPIEDADES DE LAS CONGRUENCIAS	55
4 SISTEMA COMPLETO DE RESTOS	56
6 5. SISTEMA REDUCIDO DE RESTOS	58

206 INDICE

§ 6. TEOREMAS DE EULER Y FERMAT	59
PREGUNTAS REFERENTES AL CAPITULO III	60 67
EJERCICIOS NUMERICOS REFERENTES AL CAPITULO III	07
CAPITULO CUARTO	
CONGRUENCIAS CON UNA INCOGNITA	
§ 1. CONCEPTOS PUNDAMENTALES	68
§ 2. CONGRUENCIAS DE PRIMER GRADO	69
5 3. SISTEMA DE CONGRUENCIAS DE PRIMER GRADO	71
5 4. CONGRUENCIAS DE CUALQUIER GRADO RESPECTO	73
DE UN MODULO PRIMO  5 5. CONGRUENCIAS DE CUALQUIER GRADO RESPECTO	10
DE UN MODULO COMPUESTO	75
PREGUNTAS REPERENTES AL CAPITULO IV	78
EJERCICIOS NUMERICOS REFERENTES AL CAPITULO IV	83
CAPITULO QUINTO	
CONGRUENCIAS DE SEGUNDO GRADO	
CONGREENCIAS DE SECONDO GRADO	
1. TEOREMAS GENERALES	85
2. SIMBOLO DE LEGENDRE	87
5 3. SIMBOLO DE JACOBI	92
§ 4. CASO DE UN MODULO COMPUESTO PREGUNTAS REFERENTES AL CAPITULO V	99
EJERCICIOS NUMERICOS REFERENTES AL CAPITULO V	106
EJERGIGIOS NOMERICOS REFERENTES AL CAPITOLO Y	800
CAPITULO SEXTO	
RAICES PRIMITIVAS E INDICES	
SI. TEOREMAS GENERALES	108
2. RAICES PRIMITIVAS RESPECTO DE LOS MODULOS pa Y 2pa	109
3. BUSQUEDA DE LAS RAICES PRIMITIVAS RESPECTO	
DE LOS MODULOS pa Y 2pt	111
4. INDICES RESPECTO DE LOS MODULOS pa Y 2pa	113
S B. CONSECUENCIAS DE LA TEORIA ANTECEDENTE	116
6. INDICES RESPECTO DEL MODULO 2ª	119
7. INDICES RESPECTO DE CUALQUIER MODULO COMPUESTO	122
PREGUNTAS REPERENTES AL CAPITULO VI	133
EJERCICIOS NUMERICOS REFERENTES AL CAPITULO VI	100
RESPUESTAS A LAS PREGUNTAS	
RESPUESTAS A LAS PREGUNTAS DEL CAPITULO I	135
RESPUESTAS A LAS PREGUNTAS DEL CAPITULO II	139
ALDFOLDING A DAD FALGORING DED CAFILOLO III	155
RESPUESTAS A LAS PREGUNTAS DEL CAPITULO IV	165
RESPUESTAS A LAS PREGUNTAS DEL CAPITULO V	171
RESPUESTAS A LAS PREGUNTAS DEL CAPITULO VI	101

			PIRACICIOS DEL CARITURO 1	
ESPUESTAS	A	LOS	EJERCICIOS DEL CAPITULO I	
ESPUESTAS	A	LOS	EJERCICIOS DEL CAPITULO II	
ESPUESTAS	A	LOS	EJERCICIOS DEL CAPITULO III	
ESPUESTAS	A	LOS	EJERCICIOS DEL CAPITULO IV	
ESPUESTAS	A	LOS	EJERCICIOS DEL CAPITULO V	
ESPUESTAS	A	LOS	EJERCICIOS DEL CAPITULO VI	

204

TABLA DE LOS NUMEROS PRIMOS < 4070 Y SUS RAICES

PRIMITIVAS MINIMAS

INDICE ALFABETICO DE MATERIAS

INDICE